CWID 2007 FINAL REPORT

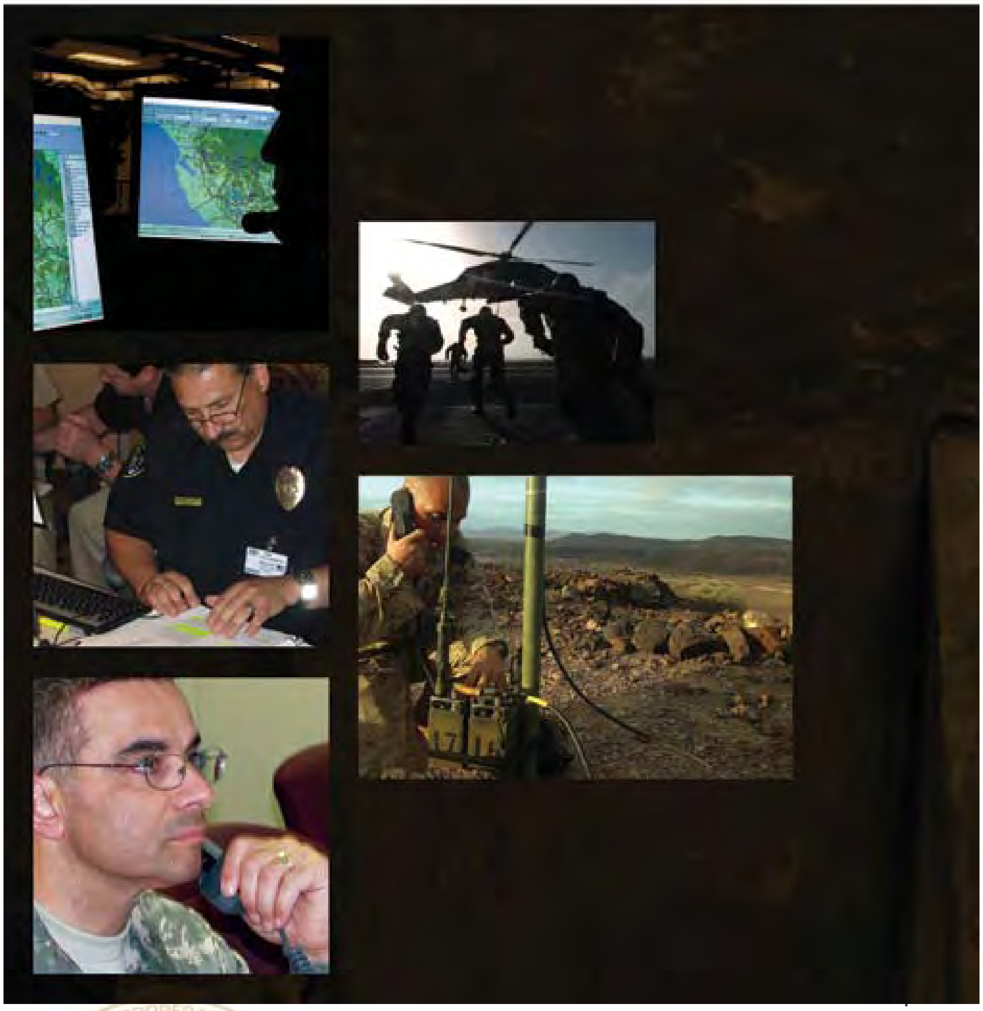
Assessment Briefs Contents

Command Endorsement

Published by: CWID JMO
Edited by: CWID JMO Hampton, VA
For information or to obtain copies, contact: CWIDPA@langley.af.mil
www.cwid.js.mil

CWID 2007 FINAL REPORT ASSESSMENT BRIEFS

Executive Summary



CWID is the Chairman of the Joint Chiefs of Staff's annual event enabling combatant commanders and the international community to investigate command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) solutions that focus on relevant and timely objectives for enhancing coalition interoperability. CWID investigates information technologies that will integrate into an operational environment within the near term following demonstration execution every year in June.

All those involved, commercial and government sectors, take some risk to realize substantial benefits. Potential technology developers bring hardware, software and package solutions to the CWID venue for assessment. Combatant commands, Services, DoD and other government agencies investigate new and emerging technologies, employing the scenario and controlled operational network for low-threat analysis.

While the focus remains new and emerging technologies, CWID 2007 was also a venue for fielded or near-fielded commercial, DoD and partner systems (those already in research and development and acquisition pipelines) to reduce costs or programmed transition timelines.

Defense Information Systems Agency (DISA) established a simulated operational network during the demonstration with participating trial assessment nodes at: Naval Surface Warfare Center, Dahlgren Division (NSWCDD), Dahlgren, VA (U.S. Army and U.S. Marine Corps site); Space and Naval Warfare Systems Command (SPAWAR), San Diego, CA (U.S. Navy site); Electronic Systems Center, Hanscom Air Force Base, MA. (U.S. Air Force site); and two combatant commander sites, U.S. European Command (USEUCOM), Stuttgart, Germany, and North American Defense - U.S. Northern Command (NORAD-USNORTHCOM), Colorado Springs, CO. Coalition partners brought more than 20 additional participants to the simulated operational network.

The CWID Senior Management Group (SMG), together with coalition partners, selected interoperability trial proposals to satisfy information sharing required among military organizations, international coalitions and civilian agencies.

One more U.S. site on the network, newly established for 2007, was located in the Pentagon. The Warfighter Capability Demonstration Center (WarCap) provided an interactive look into U.S. trial sites for senior decision makers.

Coalition participation remains the cornerstone of CWID. Interoperability trials with coalition partners were hosted over a worldwide secure network, enabling classified, releasable data exchanged among Canada, New Zealand, United Kingdom, NATO, and Partnership for Peace nations.

The CWID Senior Management Group (SMG), together with coalition partners, selected interoperability trial proposals to sat-

isfy information sharing required among military organizations, international coalitions and civilian agencies. Selection criteria is based on how well a potential trial's proposal satisfies one or more published objectives and sub-objectives.

Depending on demonstrated capabilities and based on planning-documentation criteria, each trial received one or more of three assessment types. The Systems Engineering and Integration Working Group (SEIWG), with input from other working groups, reported on interoperability trials not formally assessed by the Assessment Working Group (AWG).

The AWG is a team of three organizations. The CWID JMO consolidates and interprets Warfighter/Operator assessments of C4ISR technologies while other agencies, Joint Interoperability Test Command (JITC), under DISA, and the National Security Agency (NSA) respectively, develop assessments for Technical/Interoperability and Information Assurance. Warfighter inputs are gathered as technologies are pressed into service during the scripted scenario. Collective comments from the operations floor, interpreted for each technology, provide unusually focused insight into user interface, operational utility, training and integration issues.

U.S. Joint Forces Command (USJFCOM), on behalf of the Chairman, is responsible for oversight of CWID, a function that aligns with the command's mandate to shape future U.S. military forces.

USEUCOM is host combatant commander for CWID 2006-2008. Headquartered in Stuttgart, Germany, the command brings a native coalition emphasis. The scenario describes notional coalition task force operations applicable in any global crisis with scripted-in terrorist and natural disaster events for NORAD-USNORTHCOM's Homeland Security and Homeland Defense (HS/HD) coalition of first response partners.

CWID supported NORAD-USNORTHCOM, providing investigation of systems integration and interoperability solutions among interagency partners including the Department of Homeland Security and Public Safety and Emergency Preparedness Canada.

Strategies aimed at responsibly bringing technology solutions to the Service acquisition community are a yearly effort. CWID management is committed to information sharing solutions built on a net-centric, secure, scalable, and bandwidth-sensitive foundation.

2007 OBJECTIVES

1. CROSS-DOMAIN DATA SHARING
2. INTEGRATED INTELLIGENCE
3. INTEGRATED OPERATIONS
4. INTEGRATED LOGISTICS
5. INTEGRATED PLANNING
6. INTEGRATED COMMUNICATIONS

See expanded objectives on page 7 of this booklet

CWID demonstrations support the Network Centric Warfare construct, leveraging advantages of emerging technology.

Highlights from CWID 2007 Sites

USEUCOM

■ The host combatant command stepped forward as U.S. CWID representative to NATO CWID, bringing more direct participation at the NATO site, Lillehammer, Norway, with U.S. systems and operators. Warfighters, populating the Coalition Task Force (CTF) operations center at Kelley Barracks, Germany. Site administration functions there came from Army Liaison Teams (ALTs), USEUCOM units, unit reservists and local temporary-duty officer and enlisted support.

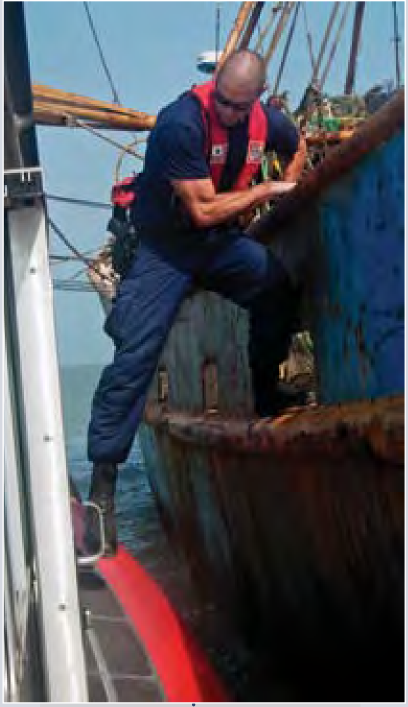
ALT teams applied a range of skilled experience in ground operations from enlisted through officer ranks. Team members hailing from Army National Guard units stationed in Colorado provided expert warfighter technology assessment input for the 2007 Final Report from recent experience in Iraq.

Another ALT unit also bridged the coalition gap for NATO, bringing "complete awareness of battlespace issues for U.S. Coalition CWID and NATO CWID," according to a NATO spokesman. The team was a palpable representation of U.S. willingness to work toward real interoperability with NATO systems.

NORAD-USNORTHCOM

■ The Homeland Security/Homeland Defense (HS/HD) site coordinated two live exercises, a hostage recovery event on home turf in Colorado Springs, CO, and a remote ship boarding with the

Coast Guard off Charleston, S.C. The CWID scenario drove civil-military response that included close cooperation between the Colorado Springs Police Department and Peterson AFB Security Police, for the second year, and with the San Diego Civil Military Operations Center (CMOC), San Diego, CA.



New Zealand connected to the HS/HD network for the first time anticipating more direct participation in 2008. They joined an already broad coalition of participants including state and bureau-level National Guard and the Canadian Government Operations Center (GOC) manned by military and civil responders including Public Safety and Emergency Preparedness Canada (PSEPC), the national equivalent of The U.S. Department of Homeland Security (DHS).

The National Guard participated at NORAD-USNORTHCOM at the Colorado Springs operations center (modeled after the NORAD-USNORTHCOM Battle Staff), the National Guard Bureau (NGB) Joint Operations Center (JOC) at the Dahlgren, VA, CWID site, and at remote live exercise sites. The Battle Staff led interactive situational awareness briefings twice daily over one trial technology that brought in additional information from NGB field exercises Palmetto CWID, Charleston, S.C., and Mountaineer CWID, WV. The West Virginia event drew in assets from all over the state and Civil Air Patrol (CAP) wings from Virginia, Maryland and Pennsylvania. All state activity involved civil first response agencies, as well as military, employing trial technologies over the CWID information network.

WARCAP

■ The first Pentagon-based site was an opportunity for those in the National Capitol Region to observe CWID from an interactive theater linked to all U.S. sites, including USEUCOM's location near Stuttgart, Germany. Some interaction from the decision-maker audience there resulted in follow-up contact with technology representatives.

CWID technologies benefit from direct interaction with senior-level organizations because operational application and/or further development requires sponsorship at some level in the acquisition community. That sponsorship can come from a single military unit or a presidential cabinet-level organization (like DoD or DHS) based on mission requirements and coordination with USJFCOM, the combatant command that is charged to equip military forces, or equivalent civil authority.

NSWC DAHLGREN

■ The U.S. Marine Corps and U.S. Army site was also host to the first CWID U.S. Coast Guard operations center and the NGB JOC for the demonstration. Marines extended their presence to a portable Command Operations Center (COC) set up outside the CWID building to simulate forward deployment. Command and control nerve centers on the CWID network reflect reality in the dual military and civil response scenario, testing operational information sharing within and between the battlespace and the homefront.

The Dahlgren-based naval operations center employed U.S. standard targeting systems with information feeds from CWID technologies. A United Kingdom and USEUCOM partnership trial and a German artillery simulation technology supported warfighter interoperability initiatives central to CWID. Closer coordination with the CWID U.S. Navy site at SPAWAR, San Diego, CA, will boost the significance of this year's success during CWID 2008.

SPAWAR

■ The U.S. Navy CWID site enjoyed increased exposure to the research and development community throughout the San Diego area in CWID 2007. Planning ahead for CWID 2008, base technology development teams and Trident Warrior exercise managers plan to participate with technologies and requirements while the San Diego Crisis Management Operations Center (CMOC) and university research teams increase their involvement with the demonstration civil response elements.

CWID 2007 demonstration highlights included wireless network infrastructure, mobile emergency communications platforms, and software protocol mesh network technology deployed in response to a scenario earthquake that simulated destruction of the San Diego county communications infrastructure. Top performing technologies from the June demonstration have been encouraged to participate in the U.S. Navy Trident Warrior exercise.

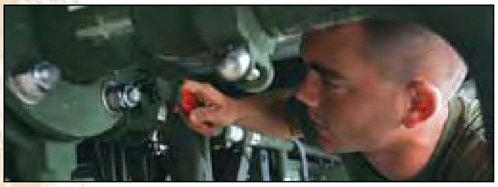
SPAWAR will continue to use CWID 2008 as a venue for existing technology development programs (Programs Of Record, or PORs) to reduce risk associated with initial operational deployments. SPAWAR's CWID site managers will also showcase coalition and civil agency interoperability by spearheading submission campaigns with the City of San Diego and local universities.

ESC, HANSCOM AFB

■ The U.S. Air Force CWID site almost tripled the number of resident trials for CWID 2007, bringing support staff to bear from Active Duty, Air Guard, Air Force Reserve and coalition countries Canada, Denmark and New Zealand. Experts from ESC units, other Hanscom AFB organizations and Massachusetts National Guard Joint Task Force Headquarters brought perspective to warfighter technology assessments straight from operations in Iraq and Afghanistan.

During CWID 2006, NEC-CCIS, a trial sponsored by the Royal Danish Air Force, enabled the U.S. Air Force to fulfill NATO C3 and USJFCOM J6 requests to issue AdatP-3 formatted air tasking and airspace control orders (ATO/ACOs). NEC-CCIS successfully imported 400-sortie ATO/ACOs and converted them from USMTF to NATO format with 100% accuracy in less than 10 minutes.

Because the technology met NATO requirements during scenario run in CWID 2006, the Joint Staff requested that the Danes provide NEC-CCIS as a core network service during CWID 2007. They supported CTF and NRF air operations seamlessly.



FROM U.S. JOINT FORCES COMMAND

Most Promising Technologies, 2007

The interoperability trials (ITs) below successfully achieved stated objectives and favorably impressed warfighters/operators and technical assessors as relevant solutions for meeting combatant command and service capability gaps.

Based on the Quicklook* responses captured during the execution phase from participating warfighters/operators, Network Operating Working Group (NOWG), Systems Engineering and Integration Working Group (SEIWG) and Site Managers/Engineers, the highlighted trials were recommended to the Senior Management Group (SMG) as the CWID Most Promising Technologies for this year's demonstration.

CWID 2007 assessed 47 trials through more than 300 scenario events.

NOTE: Trials are listed in order of trial number.

*Quicklook represents results from USJFCOM and SMG-approved surveys completed by warfighters and assessors during the demonstration. It reflects immediate detailed impressions of information technologies in the CWID operational environment. Individual detailed reports in the unabridged Final Report (on CD and online at www.cwid.js.mil) include in-depth analysis, extensive assessments and comparison of technical solutions demonstrated during CWID execution.

U.S. SPONSORED CWID TRIALS INCLUDE:

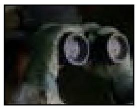
Trial No.	Title (Acronym)	Sponsor	Developer	Page
IT 1.01	Compartmented High Assurance Information Network (CHAIN)	USNORTHCOM	Raytheon	19
	MNIS candidate solution; portions of CHAIN are deployed and development continues subject to a CRADA with USJFCOM Urban Operations			
IT 1.55	Assured File Transfer (AFT)	NSA	Concurrent Technologies, Essex, Tresys Corporations	22
	Being considered for Defense IA/Security Accreditation Working Group (DSAWG) review Aug. 2008; subsequent NSA certification and agency transition			
IT 1.63	Coalition Assured Sharing Environment (CASE)	DISA	General Dynamics	24
	CASE successfully completed Trident Warrior '07 (TW07) Limited Objective Experiment, and is a candidate for TW08 to continue the PMA 160 secret and below interoperability (SABI) assessment; components in use at USPACOM			
IT 3.09	Global Personnel Recovery System (GPRS)	USJFCOM	Innovative Solutions International	28
	ACTD completed Sept. 2006, continuing under ONR supported Small Business Innovation Research (SBIR) grant; selected as a Defense Production Act project; Air Combat Command is sponsoring GPRS through the JCIDS process for USAF transition			
IT 3.27	Integrated Information Management System (IIMS)	US Air Force	U.S. Air Force	30
	Evolved from the Restoration of Operations and Contamination Avoidance at Seaports ACTD; IIMS fielded with PACAF, Osan, Republic of Korea, and USCENTCOM, Ash Shuaybah, Iraq; Joint Warrior Reporting Network (JWARN) signed a transition agreement (TA); Joint Operational Effects Federation has signed a TA with fall 2007 objective.			
IT 3.75	Mobile Tactical Edge Network (MTEN)	USNORTHCOM	Professional Software Engineering, Inc., pTerex, LLC	34
	Participated in JITC DICE Aug. 2007; beta version supports mobile connectivity requirements for the USMC Commandant; under consideration by USNORTHCOM for inclusion in the Standing Joint Forces Headquarters-North			
IT 5.08	Joint Strike Fighter Off-board Mission Support Environment (JSF OMSE)	Joint Strike Fighter Program Office	Lockheed Martin, Systematic Software Engineering, Naval Mission Planning	36
	Successfully met assessment objectives, early POR risk reduction effort; a component of the NAVAIR sponsored JSF OMSE, is the Trusted Service Engine selected for further operational assessment in TW08.			

IT 5.12	ID-MAP: Situational Awareness, Visualization and Collaboration (ID-MAP)	USNORTHCOM, US Coast Guard	General Dynamics	36
	Component of USJFCOM Warfighting Laboratory, potential for HS/HD applications; Command Post of the Future (CPOF) POR risk reduction effort			
IT 5.59	Mission Planning System (MPS)	US Air Force	Collaboration Technologies, Inc.	37
	Ongoing development planned to explore Joint Mission Planning System (USN POR) collaboration tools leading to decision to participate in CWID 2008			
IT 6.04	Tactical Emergency Asset Management (T.E.A.M.)	USNORTHCOM	Quantum Research International	38
	Mature, deployed and integrated mobile communications package; currently deployed as the primary emergency and crisis response asset in Alabama; OSD HS/HD Technology Transfer Program success story			
IT 6.53	Weapons of Mass Destruction Collaborative Advisory Response System (WMD CARS)	DTRA	DTRA	40
	GOTS equipment, risk reduction and expanded DoD exposure; POR transition plan involves implementation of WMD CARS by DTRA			
IT 6.89	Enhanced Video, Text and Audio Processing (eVITAP)	US Joint Staff	Virage, Inc.	42
	Original DARPA 2000 product currently fielded within selected U.S. and foreign governments as well as commercial news organizations; available on GSA schedule			

COALITION SPONSORED CWID TRIALS INCLUDE:

ITs described below represent coalition sponsored submissions that were demonstrated at U.S. sites or received a U.S. CWID *Quicklook assessment at an execution site outside the United States.

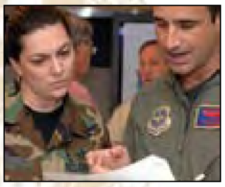
Trial No.	Title (Acronym)	Sponsor	Developer	Page
IT 1.56	Dual-Diode (One-Way) Cross-Domain Data Transfer System (Dual Diode)	Canada	Owl Computing Technologies, Inc.	23
	Successfully met planned CWID objectives; commercially available software; picked-up at SPAWAR for Spiral One development by the PMW-180 Maritime Domain Awareness (POR).			
IT 2.06	Maritime Command & Control Information System (MCCIS)	Italy	NATO ACT, Engineering Ingegneria Informatica S.p.A. Rome, IT	25
	POR demonstration; Italian T&E spiral development effort over last three years resulting in transition Fall 2007 to support maritime, ground and air COP requirements; GCCS-J compatible			
IT 3.22	Scalable Mesh Networks	US Navy	OrderOne Networks	29
	Handpicked and sponsored by SPAWAR, San Diego; highly successful demonstration selected to participate in Campaign of Experimentation including TW08 and continued development under a SBIR.			
IT 3.71	MobiKEY Identity Based Access Drive and Defense Identity Management Network (MobiKEY IBAD and DEFIMNET)	Canada	Route1, Inc.	34
	Nominated to participate in TW08; USCENTCOM C2IP candidate for Joint Staff down-select Oct. 2007			



TECHNOLOGIES TO WATCH

Based on performance and capability demonstrated during CWID, the following technologies generated high interest and warrant continued focus for potential warfighting improvement.

Trial No.	Title (Acronym)	Sponsor	Developer	Page
IT 1.17	Collaboration Gateway Collaboration Tools (CGCT)	USJFCOM, US Air Force, FBI	Trident Systems, Inc., leading more than 12 other companies	20
	POR component that used CWID 2007 to advance capability development; TW07 operational demonstration; operational test with the FBI and DHS; purchase planned for Fall 2007			
IT 3.48	Air Support Operations Center with Close Air Support System (ASOC with CASS)	US Air Force	U.S. Air Force, U.S. Navy	32
	USAF used CWID for spiral development; CASS is included in USAF POM			
IT 6.42	HotZone 4010/4020 (HZ 4010)	US Navy	Trimax Wireless, Inc.	40
	Operational in Mexico and Germany providing broadband VoIP; potential military applications supporting urban warfare communications; selected for continued operational assessment in TW08			



CWID 2007 OBJECTIVES

Objectives Drive Trial Participation

CWID 2007 charged that information sharing solutions should be built on a foundation that is net-centric, secure, scalable, and bandwidth sensitive.

CWID 2007 objectives described below contain key differences from those associated with past Joint/Coalition Warrior Interoperability Demonstrations.

Objectives are focused to reflect the following recurring themes: investigating emerging and relevant technologies; focus CWID on demonstrating solutions for combatant command theater capability gaps and challenges; enhance multi-service, multi-national, and inter-agency cooperation and communication.

OBJECTIVE

1. CROSS-DOMAIN DATA SHARING

Provide capability to share information across multiple networks of potentially different security classifications and caveats. Emphasis is on passing information to U.S. controlled, coalition networks such as Combined Enterprise Regional Information Exchange Systems (CENTRIXS) network, and coalition/alliance controlled networks such as Northern Atlantic Treaty Organization (NATO) Initial Data Transfer System (NIDTS), NATO Mission Wide Area Network. Data sharing encompasses the need for cross-domain solutions (CDS) and the assurance that information passed through CDS can be utilized by systems within all security enclaves.

■ Improve information sharing capability through secure use of operating systems and applications to facilitate battle planning and information dissemination.

1. Provide secure means for system-to-system communications across-domains.

2. Provide secure means to conduct a complete suite of collaboration activities across-domains.

3. Provide secure means for one-way and two-way file sharing across-domains to include protection from malicious code and data leakage.

4 Provide a secure intrusion detection solution for monitoring cross-domain activities.

■ Improve CDS implementation at the tactical versus operational level, recognizing that the applications are different through echelons of command.

EXPLANATION: Coalition operations require an information environment that spans multiple Communities of Interest (COI) where C/S/As are likely affected by limited bandwidth. Within any COI, mission success relates to the commander's command and control (C2) ability to communicate directly with individual users or first responders who may be detached from fixed information domains.

Objective numbering reflects approximate linkage to traditional U.S. military staff codes.

■

Objectives are supported by sub-objectives referenceing clearly defined U.S. combatant command and coalition capability gaps.

■

Objectives are linked to the Joint Battle Management Command and Control Roadmap and Joint Mission Threads.

OBJECTIVE

2. INTEGRATED INTELLIGENCE

Provide solutions that improve the commander's ability to share intelligence information products (documents, images, databases, etc.) with coalition partners, including joint and coalition forces, government agencies, NGOs, and first responders.

■ Improve rapid situational awareness of the area of operations utilizing advanced visualization technologies.

1. Demonstrate the ability to ingest geospatial data and display sophisticated 3D imagery that identifies all the elements of national resources, including political hotspots, military presence, economic icons, social, public works infrastructure, and other pertinent information.

2. Demonstrate a robust visualization architecture that supports common open application program interfaces using approved international standards and DoD approved data formats and ports/protocols.

■ Enhance the maritime common operational picture (COP) through the intelligent retrieval and fusion of data from disparate sources, population of empty track fields, analysis and detection of anomalous track behaviors and uncovering operator errors.

■ Develop customized, adaptable, dynamic, scalable intelligence estimates.

■ Develop sensor capability that automatically stores and retrieves significant events to assist the conventional forces and first responders.

■ Demonstrate fusion analysis in which computer systems and software are used to extract and compare multiple sources of information and databases.

EXPLANATION: Coalition information sharing must be secure, scaleable in scope and functional within the theater bandwidth available at all levels of warfare. Trial proposals should be capable of using existing interface standards and protocols that define the format, content, and exchange mechanisms for shared data.

OBJECTIVE

3. INTEGRATED OPERATIONS

Enhance the commander's capability to command, control, and coordinate across joint and coalition forces, government agencies, NGOs, and first responders.

- Demonstrate new technology or enhancement to existing technology that streamlines the operational decision-making process throughout the spectrum of military and civil operations, including GWOT contingencies and crisis response.
- Improved blue force tracking identification capability across multiple enclaves.
- Situational awareness using advanced visualization technologies (see Objective 2).
- Cross and secure spectrum interface capabilities for tactical/commercial radios.
- Common collaboration tool suite that is accepted by joint/conventional forces and HLS/HLD entities.
- Improved red force tracking capability across mission areas and user communities.
- Improved non-material solutions, specifically tactics, techniques, and procedures to task, discover, fuse and use Global Information Grid (GIG)-enabled products
- Shifting the focus at the operational level to long-term integration of tactical operations with specific nation-building forces and capabilities.
- Increasing tactical autonomy and decentralization.
- Providing and sharing cultural and social awareness to a level approaching situational awareness.
- Improving mobility, survivability and adaptive dominance.
- Achieving a joint/coalition integrated fire control system of systems.
- Defending effectively against the use of Electro Magnetic Pulse (EMP) or Weapons of Mass Destruction (WMD).

EXPLANATION: Integrated Operations imply that coalition, military and civilian authorities can harness the power of their respective information environments to collaboratively execute operations even in a bandwidth-constrained environment. Information exchange between these COIs must inspire confidence at each activity that the information is being disseminated securely, and will be available to agreed upon and authorized participants.

OBJECTIVE
4. INTEGRATED LOGISTICS

Demonstrate ability to access and consolidate logistical information across organizational boundaries to assess and display, in near real time, information on the movement, location and status of joint forces, military services, interagency, coalition, NGO and first responder equipment, supplies and personnel en route, and/or deployed.

- Improve logistics data access, fusion and integration among COIs.
- Improve distributed operations, operational agility, distributed support and sustainment, and exploitation of the vertical dimension of sustainment thereby reducing logistical infrastructure in-theater.

EXPLANATION: Within the information environment, the commander must have responsive and effective logistics. Logistic data is contained within diverse logistics information systems maintained by the military and civilian agencies across the coalition. Access to that data implies combining total asset visibility and information during the transit of friendly forces into a single information presentation available across multiple information COIs.

OBJECTIVE
5. INTEGRATED PLANNING

Provide solutions that improve the combatant commander's ability to conduct collaborative planning with coalition partners, including joint and coalition forces, government agencies, NGOs and first responders.

- Improve sharing capabilities that support Essential Elements of Information (EEIs) for forces supporting CTF and HLS/HLD scenarios.
- Evaluate technologies and processes that support collection and dissemination of Command and Control (C2) information using Net Centric Enterprise Services (NCES).

EXPLANATION: Integrated Planning implies that coalition, military, and civilian authorities can harness the power of their respective information environments to collaboratively plan operations even in a bandwidth-constrained environment. Collaborative planning and dissemination of products in a bandwidth constrained environment horizontally across and vertically within COIs is an emerging issue for the warfighter, particularly as software and procedure tools become sufficiently robust to be extended from the operational to the tactical level of warfare.

OBJECTIVE
6. INTEGRATED COMMUNICATIONS

Robust, joint and combined, interoperable and multilingual information sharing capabilities improve decision making and planning among Allied and coalition partners and other bandwidth-disadvantaged users.

- Translation Services: Provide solutions that improve the combatant commander's ability to share information with and receive information from multi-lingual coalition partners.
- Identify and evaluate an allied/coalition directory services architecture that facilitates the sharing of information among coalition nations.
- Create an interoperable interface between Service tactical radios and Coalition tactical radios.

1. Improve interoperability between United States Marine Crop (USMC) tactical Ultra High Frequency/Very High Frequency (UHF/VHF) radios in the frequency hopping mode and the USMC High Frequency (HF) radio with a Coalition suite of radios in the secure mode.
2. The suite of radios need to be the communication medium between the US Army Advanced Field Artillery Tactical Data System (AFATDS), the USMC AFATDS, the U.S. Navy's Naval Fire Control System, and Coalitions like system.
3. Identify and assess Voice over Internet Protocol (VoIP) solutions suitable for use over maritime tactical networks.
4. Identify National Security Agency's high assurance internet protocol encryption devices to support CDS and coalition information sharing.
5. Demonstrate domain controlled data protection at rest in a multi-domain coalition environment.
6. Demonstrate Network Defense Situational Awareness and advanced anomaly detection technologies in a multi-domain coalition environment.

EXPLANATION: Communications in a CWID context is interpreted as coalition information sharing, and is more than providing a radio communication or common operational picture at or between the strategic, operational, or tactical level of command. It must be secure, scaleable in scope and functional within the theater bandwidth available at all levels of warfare.

A MULTINATIONAL PERSPECTIVE

On-Site Interoperability Solutions

The NATO CWID programme focused primarily on testing and improving the interoperability of NATO and national C4I systems, with particular emphasis on those that would be deployed within a NATO Response Force or Combined Joint Task Force. In addition to bilateral technical testing, NATO CWID provides a venue to conduct technical testing of fielded, developmental and experimental systems in the context of a coalition scenario. The event runs concurrent and shares elements of a common scenario with the Chairman of the U.S. Joint Chiefs of Staff CWID annual event. The operational commitments for the NRFs tested in 2007 commence in July 2009 and as such, any interoperability issues that are identified as a result of trials conducted in CWID can be addressed and resolved prior to that time.

NATO CWID is well suited for the identification of interoperability shortfalls

NATO CWID offers a controlled environment where national systems, emerging technical solutions and developments of fielded systems can be evaluated and assessed to identify problems and find solutions to interoperability issues. NATO CWID provides the venue to improve NATO, national and coalition interoperability problems.

CAMP JORSTADMOEN LILLEHAMMER, NORWAY

NATO CWID EXECUTION SITE

Camp Jorstadmoen in Lillehammer, Norway hosted the NATO CWID event for 2007. The Camp has a strong military history dating back to 1750 and has been in use by the Norwegian Army Signal Corps since 1945.

During CWID execution 2004, the Camp was selected by the Norwegian parliament to be the future site of the Joint CIS Training Centre within Norway. The Camp has taken on this new role, which compliments the Joint and Coalition nature of the testing which was conducted in CWID 2007.

NETWORK ARCHITECURE

NATO CWID uses a stable, high capacity network: the Combined Federated Battle Laboratory Network (CFBLNet) in order to focus testing on the systems and services rather than the network itself

PARTICIPATING NATIONS AND SYSTEMS

There were 21 nations actively participating from the NATO execution site in Lillehammer. NATO CWID tested NRF C2 systems from each of the operational environments: the Air, Maritime and Land. The NRF Air Component structure allowed for the interoperability testing of a deployed Combined Air Operations Center (CAOC) and associated control cells. The Land Component for the NRF contained a structure sufficient to allow deployment of a tailored brigade size formation composed of manoeuvre elements and the requisite assets to allow it to conduct a wide range of land tasks. In CWID, the land component structure allowed for interoperability testing between command and control systems that use both Multilateral Interoperability Program (MIP) and ADatP-3

POINTS OF CONTACT

Cmdr. Clark Price
NATO CWID Director
ACT/C4I
cprice@act.nato.int
+1 757 445 3556

Mr. D.C. Taylor
NATO CWID Senior Analyst
ACT/C4I
dtaylor@act.nato.int
+1 757 445 3556

formats. The NRF Maritime Component was comprised of a force of multiple NATO task forces including a carrier battle group with associated surface and subsurface combat units, amphibious forces, naval MCM units and auxiliary support vessels. A force this large would not normally deploy as an NRF; however, the force was structured for interoperability testing between various maritime command and control systems.

The center column lists nations and agencies who participated in the June event at the Norwegian Joint CIS Centre of Excellence, Camp Jørstadmoen, Lillehammer, Norway.

The 2007 programme focused primarily on testing, assessing and improving the interoperability of national and NATO systems that would be deployed within a Deployed Joint Task Force (DJTF) or a NATO Response Force (NRF). These C4I systems were tested within an operational scenario and assessed for their interoperability with other C4I systems supporting the NRF or DJTF Commander. Additionally, the 2007 NATO CWID programme provided point-to-point technical testing in support of NATO and national C4I systems under development.

The NATO CWID Management Team, in conjunction with the NATO C3 Staff and JC Lisbon, developed a process whereby the testing performed at CWID would have the most operational relevance. That process began with defining the Information Exchange Requirements (IERs) that are necessary to support NRF combat operations. From these broadly worded IERs, more exact Interoperability Test Requirements (IOTRs) were created. These IOTRs – tailored to a specific combat force – apply the requirements expressed by the IERs into specific tests for the systems that support this combat force. This is in accordance with the ISC Report to the NC3B on NRF C3 Interoperability AC/322-D(2005)0050.

NATO PARTICIPANTS

Canada
Denmark
France
Germany
Italy
Netherlands
Norway
Poland
Portugal
Romania
Spain
Turkey
United Kingdom
United States

PFP PARTICIPANTS

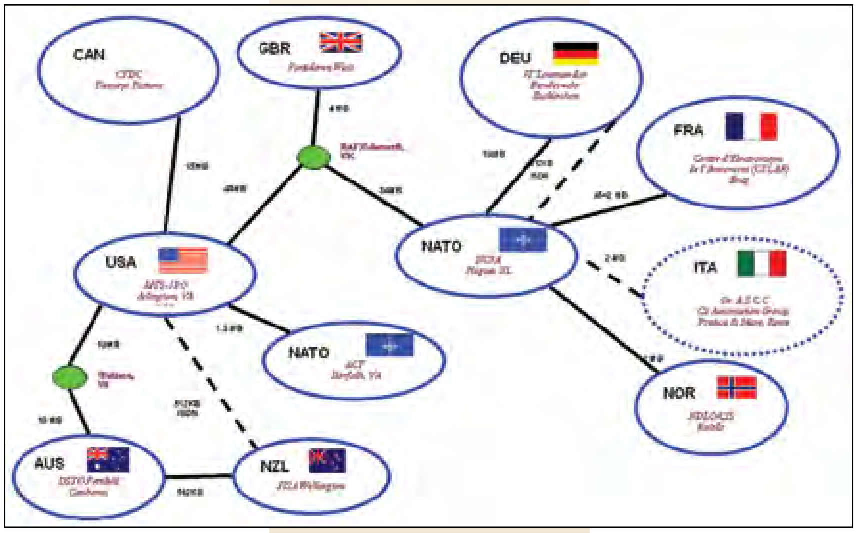
Sweden
Finland

NATO OBSERVER

Czech Republic
Estonia
Greece
Hungary

PFP OBSERVER

Austria



LAND COMPONENT COMMANDER C2 SYSTEM TESTING

Analysts from Allied Command Transformation (ACT), NIETI Core Team (NCT), Joint Warfare Centre (JWC) and Joint Air Power Competence Centre (JAPCC) were provided to support assessment and testing. The detailed results of NRF 11 and 12 system interoperability testing are contained in Chapter 5 of the full NATO CWID Final Report. This chapter reports whether the tests were successful, had limited success, had interoperability issues, or were not tested.

NATO CWID is not intended to provide battle staff training or a laboratory for wargaming through scenario play. Rather, CWID conducts testing of those C4I systems that an operational commander will be expected to use and to assess whether or not the performance of those systems, exercised within a realistic scenario, meets or exceeds the interoperability requirement.

Interoperability assessments conducted at NATO CWID are very important to the operational commander. However, of greater importance, are those systems that are found to have interoperability shortfalls while being run at NATO CWID. One of the great contributions of NATO CWID is the on-site problem solving and technology solutions generated on-the-fly by the NATO and national system engineers that are present. The added value of having such technical expertise from diverse backgrounds working physically side by side cannot be over emphasized.

Although NATO and its coalition partners are clearly more interoperable today than we have ever been, interoperability currently falls short of the NRF CIS interoperability requirement. Resolution of the interoperability challenges needs the active involvement of Nations and all levels of the NATO Command structure under a coordinated program. NATO CWID is well suited for the identification of interoperability shortfalls.

THE ASSESSMENT PROCESS

Three-Pronged Expert Assessment

The Assessment Working Group's (AWG) charter is to provide the Joint Staff, Combatant Commands/Services/Agencies (C/S/A), and other interested parties with an objective assessment of warfighter/operator utility, interoperability, and Information Assurance (IA) for Interoperability Trials (ITs).

THE ASSESSMENT PROCESS

The assessment effort's overarching goal is to identify potential candidates that provide C4I interoperability capabilities or enhancements to Joint, Coalition, and Homeland Security/Homeland Defense (HS/HD) operations.

The AWG consists of three distinct teams, the Warfighter/Operator Utility Assessment Team, the Interoperability/Technical Assessment Team and the Information Assurance Assessment Team. Each team is responsible for assessing a different aspect of the trial as it operates within the CWID environment. These teams consist of C4ISR Analysts who perform the military utility, interoperability assessments and Information System Security Engineers and Security Testing Specialists, who assess the trial's IA posture.

The assessment teams independently review each trial to determine the trial's nature, maturity level, and technical factors to define the appropriate level of assessment each trial receives. In addition, the teams consider the Senior Management Group's (SMG) tri-al prioritization list when determining how best to apply the AWG's limited resources.

During CWID's planning and execution phases, the assessment teams and IT representatives work cooperatively to ensure that ITs receive objective and meaningful assessments. The assessments include inputs from operational users and the assessment teams' analysts, testers, and observers. The results, captured in various database views and team summaries, documents how well ITs satisfy applicable CWID objectives in the context of warfighter/operator utility, interoperability, and information assurance.

The overarching goal of the assessment effort is to identify potential candidates to provide C4I interoperability capabilities or enhancements to Joint, Coalition, and Homeland Security/Homeland Defense operations.

WARFIGHTER/OPERATOR UTILITY ASSESSMENT PROCESS

The Warfighter/Operator Assessment focused on the "value added" to warfighters and operators, trial technical performance, and the trial's ability to meet objectives and capabilities in the operational CWID environment.

During CWID execution, warfighters, operators and staff interacted with trials, evaluating system utility by completing CWID network accessible questionnaires generated via the Joint Systems Integration Command (JSIC) Data Collection and Analysis Tool (JDCAT). Questionnaires were intended to collect feedback and other data to evaluate the usefulness, effectiveness, suitability, and performance of the system. These parameters attempted to capture the degree that a system enhances the warfighter's mission operational performance and the systems capability and capacity to support task completion in a timely manner. Inherent in these attributes were Measures of Performance (MOPs) such as information accessibility, accuracy, adaptability, consistency, and relevancy.

Data required for each IT's assessment was defined prior to execution based on:

- How the IT's capabilities map to CWID objectives
- Predefined Master Scenario Events List (MSEL) events and/or definitive test schedules
- Trial capabilities
- MOPs tailored for each trial

INTEROPERABILITY ASSESSMENT PROCESS

The Interoperability/Technical Assessment focused on an IT's ability to exchange usable data with CWID network services or other trials. During CWID planning, the Interoperability Assessment Team worked with each trial's representatives to define Information Exchange Requirements (IER) based upon system interfaces, anticipated data exchanges, and their mapping to CWID objectives. IERs define what information is exchanged, who exchanges the information, why the information is necessary, and how the exchanges take place.

During execution, the Interoperability Assessment Team observed whether or not data was transferred to, and processed correctly by the receiving system. Results were documented in the JITC's WISE Interoperability Collection Assessment Tool (WICAT) database. Applicable portions of this database are delivered to the trials during the reporting phase. All information collected by the Interoperability Assessment Team can support the formal U. S. Interoperability Certification Process, potentially expediting product fielding.

INFORMATION ASSURANCE ASSESSMENT PROCESS

The IA Team performs varying analysis levels during CWID's planning, execution, and reporting phases. During the planning phase, the team performed an analysis of the trials' capabilities to determine an appropriate assessment level for each trial. Trials were eligible to receive one of three types of IA Assessments: Basic, Conceptual, or Targeted.

The Assessment Working Group is comprised of three separate analyst teams that provide three different categories of assessments:

■

Warfighter/Operator Utility

■

Interoperability/ Technical

■

Information Assurance

Trials that connected equipment to select CWID networks during execution received a Basic Assessment; a simple, non-intrusive discovery scan using tools such as Retina, Nessus, Network Mapper (NMAP), and Kismet.

The IA Conceptual Assessment was performed on U.S.-Sponsored trials with IA functionality that were only virtually connected to U.S. sites. The Conceptual Assessment, intended to bring information security awareness to the vendor, recorded and analyzed the vendor's information security claims. Conceptual Assessments resulted from a paper study completed suring the planning process.

The Targeted Assessment provided analysis of the Conceptual Assessment, while also utilizing testing and discovery tools to substantiate the vendor's claims. In theory, it was a combination of all activities of the Conceptual and Basic Assessments.

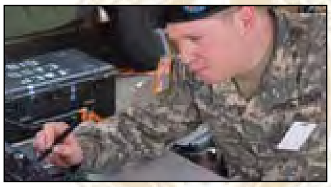
Selected trials were reviewed and inspected for particular IA capabilities and threats to which they might be vulnerable.

Data collected during execution shaped the IA Team's input to the Final Report. IT vendors can use the results of the IA Assessment to garner a sense of their product's security posture.

CWID EXECUTION

During execution, AWG members were on-site at USEUCOM, USNORTHCOM, NSWC Dahlgren VA, SPAWAR San Diego CA, Hanscom AFB, MA. Additionally, Canada, NATO, New Zealand and United Kingdom also provided on-site assessment support to help collect trial data and evaluate trial performance at their site.

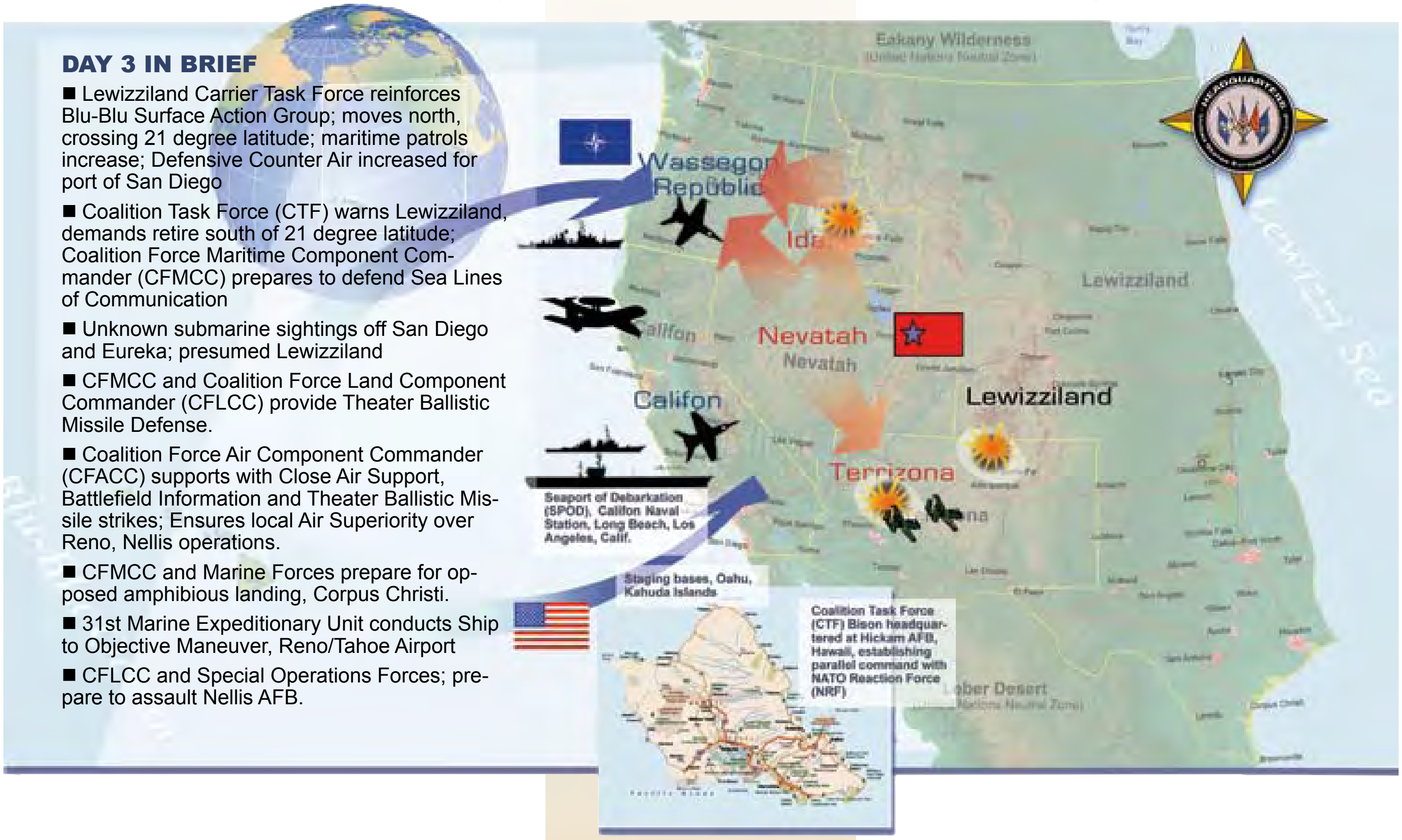
Forty-six trials participated in CWID 2007 and received various levels of assessment from the three pronged warfighter/operator, technical interoperability, and information assessment process. Specifically, 37 trials received a Warfighter Assessment, 32 received an Interoperability Assessment, 36 received an Information Assurance assessment, and three trials received a conceptual information assurance assessment. SEIWG reported on 11 trials.



TWO-PART SCENARIO

Scripted Environment for Technology Trials

The scenario described notional coalition task force operations applicable in the current environment with terrorist backlash and natural disasters for North American Defense - U.S. Northern Command's (NORAD-USNORTHCOM) Homeland Security and Homeland Defense (HS/HD) component. The simulated operational environment provided context for validation of proposed technology solutions.


Eakany Wilderness
(United Nations Neutral Zone)
HEADQUARTERS
Wassegon Republic
Ida
Nevatah
Nevatah
Califon
Califon
Lewizziland
Lewizziland
Terrizona
Lewizzi Sea
Seaport of Debarkation (SPOD), Califon Naval Station, Long Beach, Los Angeles, Calif.
Staging bases, Oahu, Kahuda Islands
Coalition Task Force (CTF) Bison headquartered at Hickam AFB, Hawaii, establishing parallel command with NATO Reaction Force (NRF)
ober Desert
(United Nations Neutral Zone)

DAY 3 IN BRIEF

- Lewizziland Carrier Task Force reinforces Blu-Blu Surface Action Group; moves north, crossing 21 degree latitude; maritime patrols increase; Defensive Counter Air increased for port of San Diego
- Coalition Task Force (CTF) warns Lewizziland, demands retire south of 21 degree latitude; Coalition Force Maritime Component Commander (CFMCC) prepares to defend Sea Lines of Communication
- Unknown submarine sightings off San Diego and Eureka; presumed Lewizziland
- CFMCC and Coalition Force Land Component Commander (CFLCC) provide Theater Ballistic Missile Defense.
- Coalition Force Air Component Commander (CFACC) supports with Close Air Support, Battlefield Information and Theater Ballistic Missile strikes; Ensures local Air Superiority over Reno, Nellis operations.
- CFMCC and Marine Forces prepare for opposed amphibious landing, Corpus Christi.
- 31st Marine Expeditionary Unit conducts Ship to Objective Maneuver, Reno/Tahoe Airport
- CFLCC and Special Operations Forces; prepare to assault Nellis AFB.

COALITION TASK FORCE SCENARIO

U.S. European Command (USEUCOM) was the host Combatant Command for Coalition Warrior Interoperability Demonstration (CWID) 2007. The conflict notionally occured on a land mass and littoral of USEUCOM's area of responsibility (actually Western Continental United States for planning and mapping purposes). A U.S.-led CTF and a NATO joint force, NATO Reaction Force (NRF), comprised friendly forces. The friendly island nation of Kahuda (actually Hawaii) agreed to provide basing for interim staging and logistical requirements. The CWID 2007 scenario's theme began with a pre-existent, moderate-sized Terrizona Stabilization Force conducting stabilization operations in one nation. Regional unrest then escalated to a regional

MAJOR EVENTS WHEN THE SCENARIO STARTS

- **Candian and Italian-led Terrizona Stabilization Force (TSF) in place, Terrizona.**
- CTF Bison is in theater, Oahu, Kahuda Islands; forces marshaled; limited deployment into Area of Operations (southern Califon,Terrizona).
- NRF emplaced in area of operations (Wassegon).

DISTRIBUTED TASK FORCE ELEMENTS

COALITION TASK FORCE

U.S. EUROPEAN COMMAND (USEUCOM): Combatant Command; Coalition Task Force Commander; role plays out of Kelley Barracks, Stuttgart, Germany.

COALITION LAND COMPONENT COMMANDER (CFLCC): role plays out of Naval Surface Warfare Center (NSWC), Dahlgren, VA; U.S. Army and U.S. Marine Corps elements of the CFLCC role play out of NSWC, Dahlgren, VA.

COALITION FORCE MARITIME COMPONENT COMMANDER (CFMCC): role plays out of Space and Naval Warfare Systems Command (SPAWAR), San Diego, CA.

COALITION FORCE AIR COMPONENT COMMANDER (CFACC): role plays out of Electronic Systems Center (ESC), Hanscom Air Force Base, MA.

NATO RESPONSE FORCE

Command elements of NRF role play out of Camp Jorstadmoen, Lillehammer, Norway

NATIONAL ELEMENTS

Canada, New Zealand, and the United Kingdom role play units from their respective countries; Canada role plays homeland defense with NORAD-US-NORTHCOM, Colorado Springs, CO.

multinational insurgency, cross-border invasion and mid-intensity conflict. Destabilization, humanitarian crisis, and hostilities required the deployment of coalition task forces to reinstate regional stability.

HOMELAND SECURITY/HOMELAND DEFENSE SCENARIO

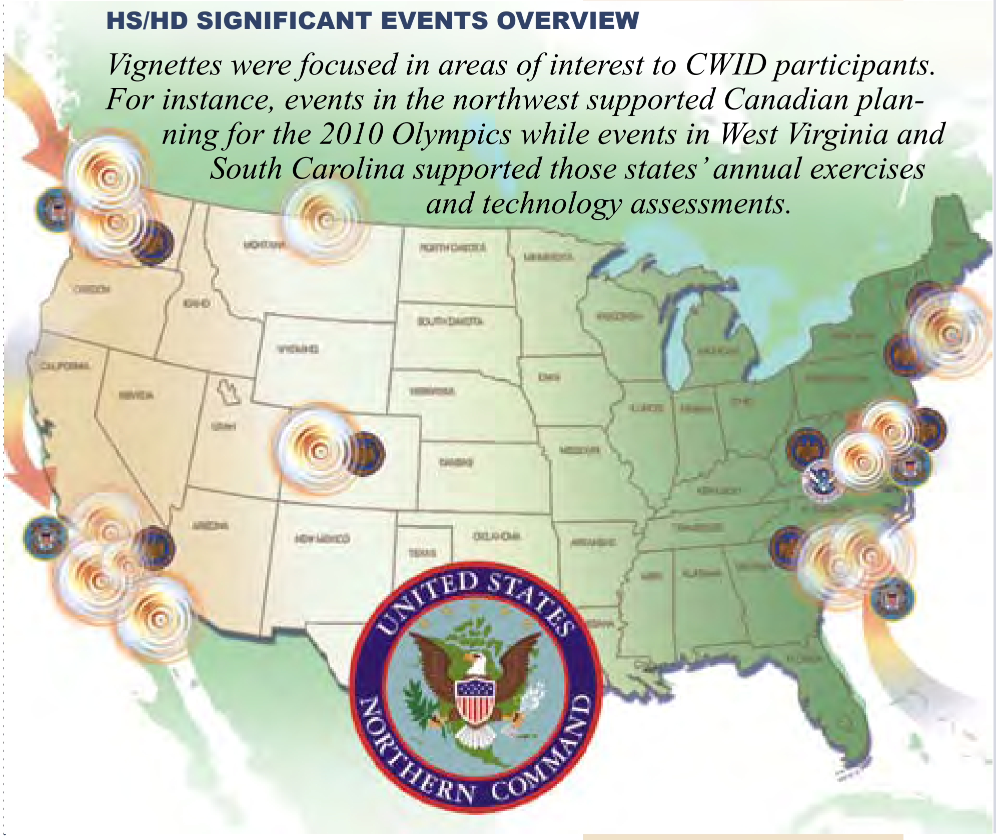
The HS/HD scenario exploited an ongoing interest in technologies that support global, civil, and/or natural disasters with terrorist backlash and information sharing between military forces and federal, state and local governments. The HS/HD scenario consisted of several vignettes within NORAD-USNORTHCOM's Area of Responsibility (AOR). Scenario vignettes provided a broad spectrum of natural and terrorist-related events.

Vignettes were focused in areas of the AOR of interest to CWID participants. For instance, events in the northwest supported Canadian planning for the 2010 Olympics while events in West Virginia and South Carolina supported those states' annual exercises and technology assessments.

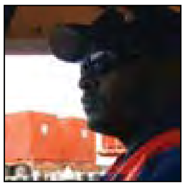
THE HOMELAND DEFENSE MISSION included participation by USNORTHCOM; U.S. Coast Guard; National Guard Bureau; National Guards of California, Colorado, Delaware, Massachusetts, New York, South Carolina and West Virginia; Department of Justice Seahawk Center; Canada Command; Canadian Government Operations Centre; Canadian Mapping and Charting Establishment; government intelligence liaison officers from both the U.S. and Canada; and the police departments of the cities of San Diego and Colorado Springs.

HS/HD SIGNIFICANT EVENTS OVERVIEW

Vignettes were focused in areas of interest to CWID participants. For instance, events in the northwest supported Canadian planning for the 2010 Olympics while events in West Virginia and South Carolina supported those states' annual exercises and technology assessments.



- ■ Mass evacuation from Northern Virginia area into West Virginia, surrounding states
- ■ Earthquake, San Diego, CA.
- ■ Hurricane preparation; landfall, Charleston, S.C.
- ■ Chemical release, NSWC Fallbrook, CA,
- ■ Merchant ships missing; one found off San Diego with 10kt nuclear device; one found off Charleston, launching cruise missile at city
- ■ Fuel spill, Potomac River
- ■ Attack on refinery; state of Washington
- ■ Anthrax attacks at train stations, Vancouver, BC, and Seattle, WA.
- ■ Chemical weapon explosion, rail station, Fredericksburg, VA.
- ■ Radiological dispersion device (RDD) threat, San Diego; RDD detonation, Boston, MA.
- ■ Man Portable Air Defense threats, San Diego, Seattle, Vancouver
- ■ Truck bombs at power plant, Virginia; PETCO Park, San Diego
- ■ Suspicious ship activity, port of Charleston
- ■ Wildland fires, San Diego; along U.S., Canada border
- ■ Mass evacuation from Mexico as a result of a plague outbreak
- ■ Hostage situation, Colorado Springs, CO; high ranking NORAD-USNORTHCOM official



NETWORK ENGINEERING SUMMARY

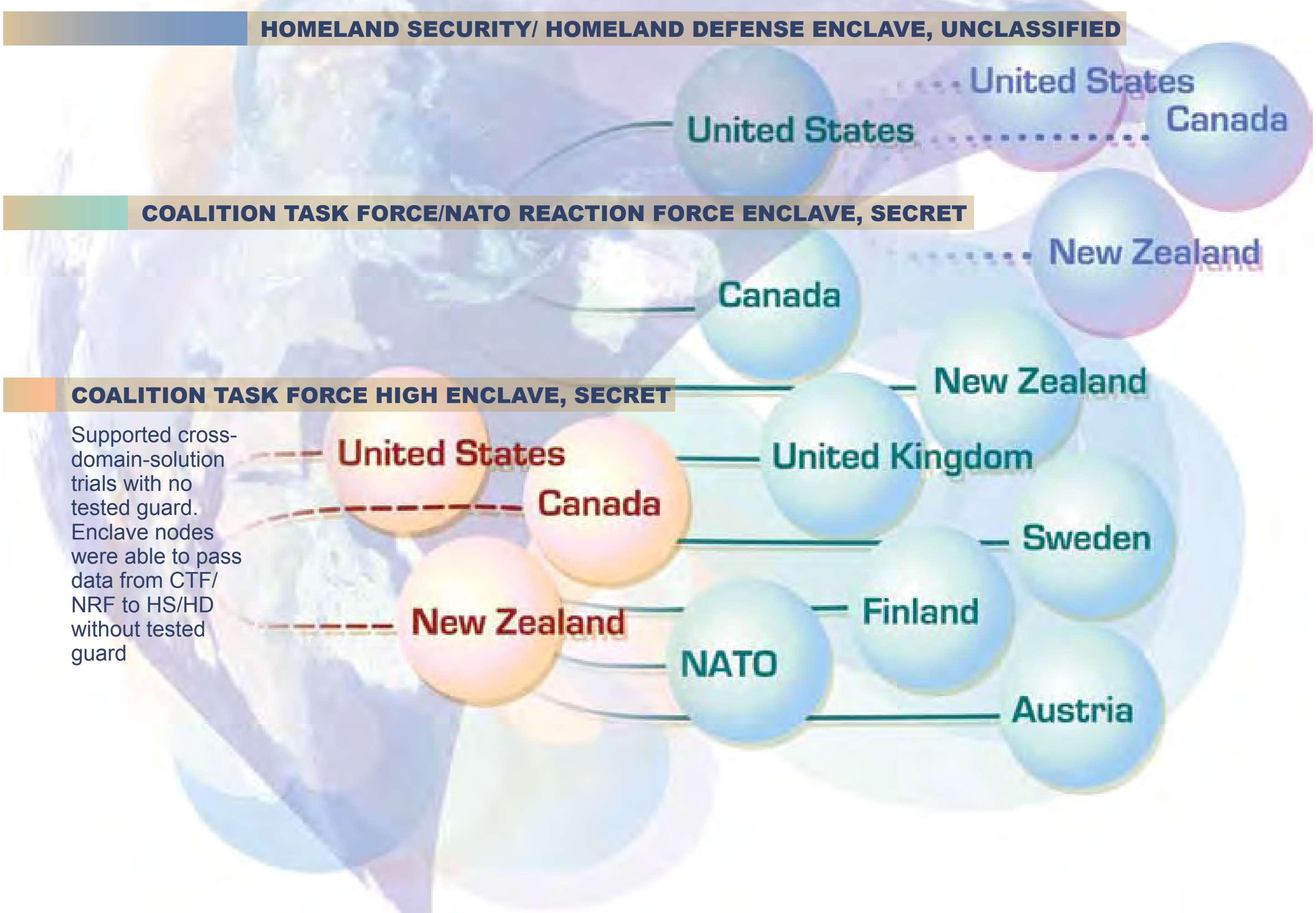
A Dynamic, Three-Enclave Network

The CWID network was a dynamic environment which included several CWID firsts. Engineers created three security enclaves: the Homeland Security/Homeland Defense (HS/HD), unclassified; Coalition Task Force/NATO Reaction Force (CTF/NRF), secret; and the CTF High, secret enclave, a notionally higher classification than CTF/NRF. The CTF High enclave supported cross-domain-solution trials that did not use a tested guard, so were unable to pass data from CTF/NRF to HS/HD.

Another new addition to CWID was Internet connectivity with public e-mail addresses for the HS/HD enclave, greatly increasing support provided to NORAD-USNORTHCOM and their HS/HD community.

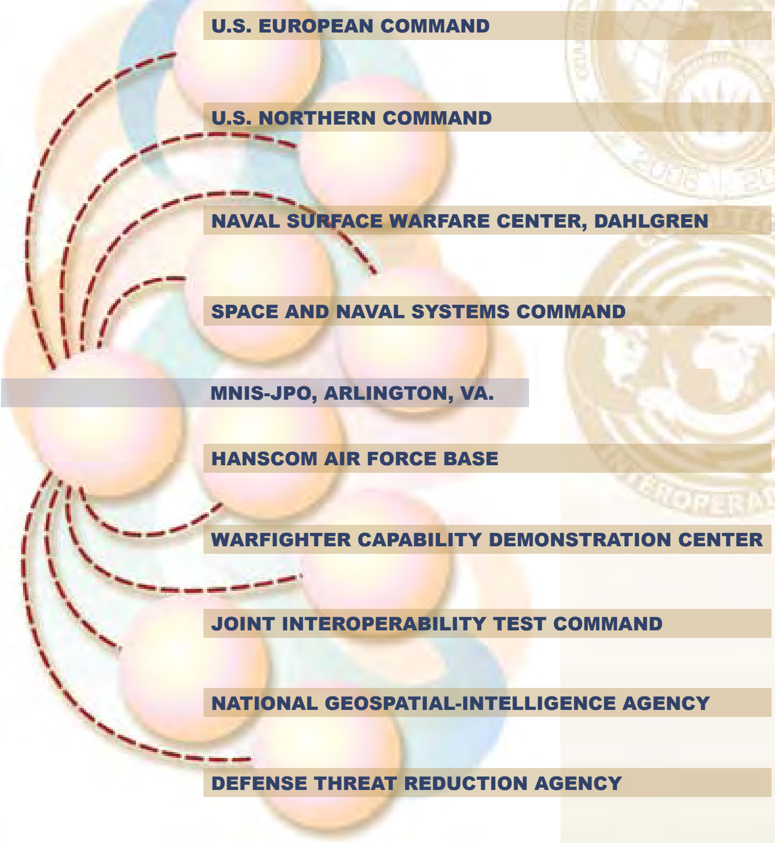
Network engineers used the Combined Federated Battle Laboratories Network (CFBLNet) as the backbone, utilizing type-1 encryption to separate enclaves. They designed the network to be scalable, flexible and to closely emulate current operational networks while still providing a low threat environment

THREE SECURITY ENCLAVES


HOMELAND SECURITY/ HOMELAND DEFENSE ENCLAVE, UNCLASSIFIED
United States
United States
Canada
COALITION TASK FORCE/NATO REACTION FORCE ENCLAVE, SECRET
New Zealand
Canada
COALITION TASK FORCE HIGH ENCLAVE, SECRET
New Zealand
United States
Canada
United Kingdom
Sweden
New Zealand
Finland
NATO
Austria

Supported cross-domain-solution trials with no tested guard. Enclave nodes were able to pass data from CTF/NRF to HS/HD without tested guard

U.S. NETWORKED SITES


U.S. EUROPEAN COMMAND
U.S. NORTHERN COMMAND
NAVAL SURFACE WARFARE CENTER, DAHLGREN
SPACE AND NAVAL SYSTEMS COMMAND
MNIS-JPO, ARLINGTON, VA.
HANSCOM AIR FORCE BASE
WARFIGHTER CAPABILITY DEMONSTRATION CENTER
JOINT INTEROPERABILITY TEST COMMAND
NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY
DEFENSE THREAT REDUCTION AGENCY

to demonstrate and assess new technologies.

Another first, engineers integrated Symantec Corporation's Deep Sight network defense system to secure the infrastructure. CWID network users employed a variety of of the comany's products for virus scanning and mail filtering, provided under DoD enterprise license.

The core of the CWID network resided at the Multinational Information Sharing-Joint Program Office (MNIS-JPO) facility in Arlington, VA. Network engineers manned a Coalition Communications Control Center from where they monitored network health and performance and assisted network users.

A notable achievement for CWID 2007 was the 100% availability of the network backbone throughout the 2-week execution period.

CWID networks are designed to be scalable, flexible and to closely emulate operational networks.

THE CTF/NRF ENCLAVE

The CTF/NRF Enclave utilized the CFBLNet Backbone Asynchronous Transfer Mode transport layer. Designed as a secret-releasable network for all network participants, it was capable of supporting high-speed data transmission of up to 45Mbps. In the U.S., the CTF/NRF enclave shared up to 40 Mbps bandwidth with other enclaves. The CTF/NRF enclave connected eight U.S. and five Coalition sites.

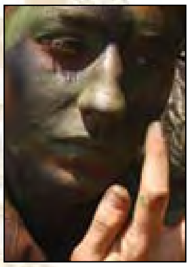
Network core services such as Domain Name Service, network timing, anti-virus signature updates and collaboration portal, were provided by multiple countries, creating an actual coalition network environment.

THE HS/HD ENCLAVE

The HS/HD enclave shared CFBLNet transport with the CTF/NRF enclave, but only supported unclassified data. This enclave, established to support NORAD-USNORTHCOM's participation, connected all sites in the continental U.S. and one in Germany (U.S. European Command, USEUCOM).

Engineers provided Internet connectivity via dual T-1 connections (3 Mbps) over public telephone services. They also provided public e-mail, using Symantec's SMTP Gateway as a filter.

Extensive use of 256-bit Advanced Encryption Standard encrypted Virtual Private Network tunnels allowed public first-responder participation, to include police, firefighters and National Guard operations centers. Canada and New Zealand also accessed the CWID HS/HD infrastucture.



TRIALS CONTENTS PAGE

Interoperability Trials

Coalition Warrior Interoperability Demonstration trials for 2007 are listed in trial number order below, cross referenced to sites where they were observed during the demonstration June 18 to 21.

OBJECTIVES KEY

1. CROSS-DOMAIN DATA SHARING ■
2. INTEGRATED INTELLIGENCE ■
3. INTEGRATED OPERATIONS ■
4. INTEGRATED LOGISTICS ■
5. INTEGRATED PLANNING ■
6. INTEGRATED COMMUNICATIONS ■

TRIAL NO.	SYSTEM TITLE (ACRONYM OR SHORT NAME)	USEUCOM	USNORTHCOM	DAHLGREN	SPAWAR	HANSCOM	CANADA	NEW ZEALAND	UNITED KINGDOM	NATO	GOVERNMENT SPONSOR	GOVERNMENT/ CORPORATE DEVELOPER/S	OBJECTIVE/S ADDRESSED	PAGE NO.
1.01	Compartmented High Assurance Information Network (CHAIN)	■	■	■	■	■					USNORTHCOM	Raytheon	**1**,3,4,5	19
1.05	Trusted Gateway System (TGS) Guard				■	■		■			US Air Force	US Air Force	**1**	19
1.17 **1.17A**	Collaboration Gateway (CG) Collaboration Gateway Collaboration Tools (CGCT)		■	■	■	■					US Air Force, USJFCOM, FBI	Trident Systems, Inc., leads more than 12 other companies	**1**,2,3,5	20
1.28	NET/X eToken Security System, Deployable Communicartions System (NET/X)		■	■	■						USJFCOM	FED-COMM USA, Inc.	**2**	21
1.43	Mobile Forces Solution - Subnet Relay (MOFS-SNR)				■					■	Germany	T-Systems Enterprise Services GmbH	**1**	21
1.54	Collaborate-Access-Browser (CAB)	■	■	■	■	■		■			NSA	Essex Corporation	**1**	22
1.55	Assured File Transfer (AFT)	■		■	■	■		■			NSA	CTC, Essex Corporation,Tresys Technology	**1**	22
1.56	Dual Diode (One-Way) Data Transfer System (Dual Diode)				■		■	■			Canada	Owl Computing Technologies, Inc.	**1**	23
1.61	INTEGRITY Secure Workstation (INTSecWS)						■				Canada	Green Hills Software, Inc.	**1**	23
1.63	Coalition Assured Sharing Environment (CASE)		■	■							DISA	General Dynamics	**2**	24
1.86	Federated Identity Mangement System (FIDMS)		■	■		■					USJFCOM	BearingPoint, Hewlett Packard	**1**	24
1.87	Federated Security (FS)			■							USJFCOM	SAIC, IBM, Sun	**2**	25
2.06	Italian Navy Maritime Command and Control Information System (MCCIS-Italy rel. 5.2)				■					■	Italy	MARITEL-Roma	**2**	25
2.16	Deployable Geospatial Database (DGDB)		■				■				Canada	Canada	**2**	26
2.21	Commercial Joint Mapping Tool Kit (CJMTK)		■	■	■				■		NGA	Northrop Grumman Corporation	**2**	26
2.37	Rapid Force Warning (RFW)					■				■	US Air Force	US Air Force	**2**	27
2.57	Automatic Ingest, Mosaic and Mapping System (AIMM)		■	■	■		■				Canada	PCI Geomatics.	**2**	27
2.88	AdLib			■					■		USNORTHCOM	EchoStorm, Inc.	**2**	28
3.09	Global Personnel Recovery System (GPRS)	■	■	■							USJFCOM	Innovative Solutions International	**2**,3,4,5	28
3.14	Coalition Secure Management and Operations System (COSMOS)	■		■			■		■	■	OSD, USEUCOM, DISA	DISA, NSA, CDM	**3**,6	29
3.22	Scalable Mesh Networks				■						US Navy	OrderOne Networks	**3**,2	29
3.27	Integrated Information Management System (IIMS)			■							US Army, US Air Force	US Army, US Air Force	**3**	30

Continued next page

OBJECTIVES KEY

1. CROSS-DOMAIN DATA SHARING ■
2. INTEGRATED INTELLIGENCE ■
3. INTEGRATED OPERATIONS ■
4. INTEGRATED LOGISTICS ■
5. INTEGRATED PLANNING ■
6. INTEGRATED COMMUNICATIONS ■

TRIAL NO.	SYSTEM TITLE (ACRONYM OR SHORT NAME)	USEUCOM	USNORTHCOM	DAHLGREN	SPAWAR	HANSCOM	CANADA	NEW ZEALAND	UNITED KINGDOM	NATO	GOVERNMENT SPONSOR	GOVERNMENT/ CORPORATE DEVELOPER/S	OBJECTIVE/S ADDRESSED	PAGE NO.
3.30	Spatio-Temporal Analysis for Rapid Tasking (START)					■					US Air Force	The MITRE Corporation	**3**	**30**
3.31	Coalition Infrared Data Processing (CIDP)	■		■					■		US Air Force	Space and Missile Center, Missile Defense Agency	**3**,5	**31**
3.38	Collaborative Decision Aid (CDA)		■	■							NGB	ARINC Engineering Services, LLC	**3**,5	**31**
3.39	Command, Control, Communications, Computers and Intelligence Defence (C4I Defence)	■		■		■	■				Italy	SELEX-SI SpA	**3**	**32**
3.48	Air Support Operations Center with Close Air Support System (ASOC Gateway with CASS)			■							US Air Force	US Air Force, US Navy	**3**	**32**
3.58	US Coast Guard Information Sharing and Communications (USCG IS&C)		■	■							US Coast Guard	US Coast Guard	**3**	**33**
3.70	Coalition open Joint Operations Picture (CoJOP)	■		■	■	■	■	■	■		UK	Fujitsu Services	**3**,5	**33**
3.71	MobiKEY Identity Based Access Drive (MobiKEY IBAD) and Defense Identity Management Network (DEFIMNET)	■	■	■	■	■	■	■			Canada	Route1, Inc.	**3**,5	**34**
3.75	Mobile Tactical Edge Network (MTEN)		■	■							USNORTHCOM	Professional Software Engineering, Inc., pTerex, LLC	**3**	**34**
3.80	Riverbed Information Optimization System (RIOS)	■		■		■		■			US Air Force, DISA	C2I Solutions, Riverbed	**3**,4	**35**
4.79	Event-based Common Operational Picture (ECOP)		■	■	■	■					NGB	Booz Allen Hamilton	**3**,4,5	**35**
5.08	Joint Strike Fighter (JSF) Offboard Mission Support Environment (OMSE)			■		■			■		JSF Program Office	Lockheed Martin, Systematic Software Engineering, Naval Mission Planning	**5**,1	**36**
5.12	ID-MAP: Situational Awareness, Visualization and Collaboration (ID-MAP)		■	■	■						USNORTHCOM, US Coast Guard	General Dynamics	**5**,2,3	**36**
5.59	Mission Planning System (MPS)					■	■	■			US Air Force	Collaboration Technologies, Inc.	**3**,5	**37**
5.78	Next Generation - Joint Information Exchange Environment (NG-JIEE)		■	■	■	■					NGB	Koniag Services, Inc.	**5**	**37**
6.04	Tactical Emergency Asset Management (T.E.A.M.)		■		■						USNORTHCOM	Quantum Research International	**6**	**38**
6.13	Global Information Grid Quality of Service Edge Solution for Interoperability (GIG QoS ESI)			■	■			■			US Army	DSCI	**6**	**38**
6.15	Geolap		■				■		■		Canada	Canada	**6**	**39**
6.36	Joint Network Defense and Management System (JNDMS)						■				Canada	MacDonald Dettwiler and Associates (MDA)	**6**	**39**
6.42	HotZone 4010/4020 (HZ4010)				■						US Navy	Trimax Wireless, Inc.	**3**,6	**40**
6.53	Weapons of Mass Destruction Collaborative Advisory Response System (WMD CARS)	■	■		■	■					USNORTHCOM	Defense Threat Reduction Agency (DTRA)	**3**,5	**40**
6.66	Internet Protocol Interoperability and Collaboration System (IPICS)		■	■			■				Canada	Cisco Systems, Inc.	**6**	**41**
6.74	Security Information Management for Enclave Networks (SIMEN)		■	■		■		■			US Air Force	The MITRE Corporation	**1**,6	**41**
6.89	Enhanced Video Text and Audio Processing (eVITAP)		■	■	■		■	■			US Joint Staff	Virage Inc.	**6**	**42**
6.90	Optimized Data Environment for NetCentric Operations (ODEN)	■	■	■	■						USCENTCOM	TIMMES, Inc.	**6**	**42**
History of Coalition Warrior Interoperability Demonstration														**43**
Trial Highlights, 2005 and 2006														**44**
Abbreviations and Acronyms, inside back cover														

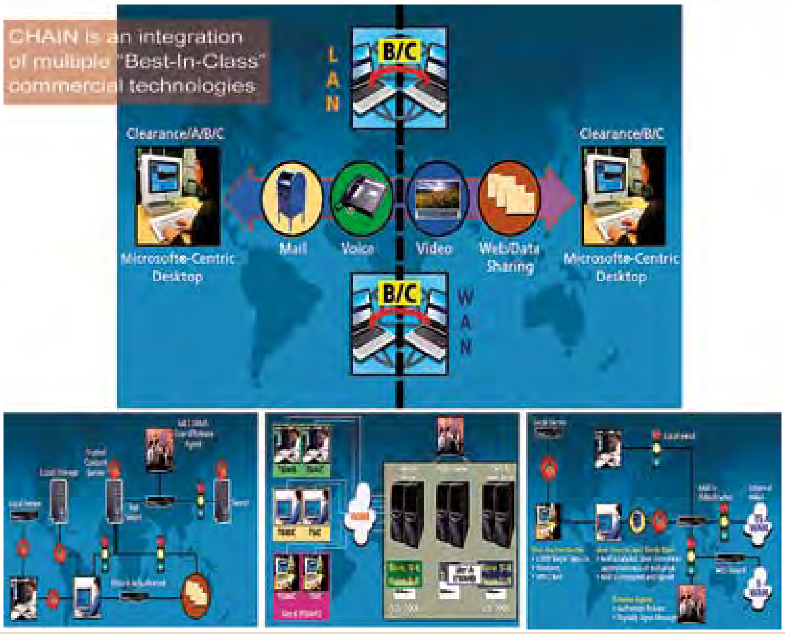
IT 1.01 UNABRIDGED ASSESSMENT LINK

Compartmented High Assurance Information Network

1. CROSS-DOMAIN DATA SHARING ● 3. INTEGRATED OPERATIONS ● 4. INTEGRATED LOGISTICS ● 5. INTEGRATED PLANNING ●

TRIAL OVERVIEW: CHAIN is a windows-based solution, not a product, for multi-compartmented secure interoperability in Joint and Coalition Operations. The architecture is a combination of Windows based servers and workstations, and various COTS applications enhanced for advanced security. CHAIN provides compartmented email, trusted content server capabilities, and security enhanced collaboration tools while capitalizing on existing user's skill sets. CHAIN allows users to share data, white board and chat within their own community of interest, as well as expand or limit access based on the sensitivity of the discussion, access and security level.

SPONSOR:
USNORTHCOM
LOCATIONS:
USEUCOM
USNORTHCOM
NSWC Dahlgren
SPAWAR
ESC Hanscom
PARTNERS:
none


CHAIN is an integration of multiple "Best-In-Class" commercial technologies
L A N
B/C
Clearance/A/B/C
Clearance/B/C
Microsofte-Centric Desktop
Mail
Voice
Video
Web/Data Sharing
Microsofte-Centric Desktop
B/C
W A N

ASSESSMEMT RESULTS::
During CWID 2007, the CHAIN Trial operated on the CTF and HS/HD domains and received Warfighter, Technical Interoperability and Basic Information Assurance (IA) assessments.

- CHAIN successfully met CWID objectives 1, 3, 4 and 5 by providing the ability to securely share near real-time data and voice transmissions among disparate communities of interest (COIs). CHAIN facilitated creating and modifying a progressive conference with users in different security domains where at least one common level between the two existed.

- CHAIN successfully denied calls between incompatible security domains and demonstrated the Compartmented Email function where the user was authenticated at the desktop.

- CHAIN's effective determination of security caveats and use of security measures improved information sharing while preserving the integrity of Essential Elements of Information (EEIs).

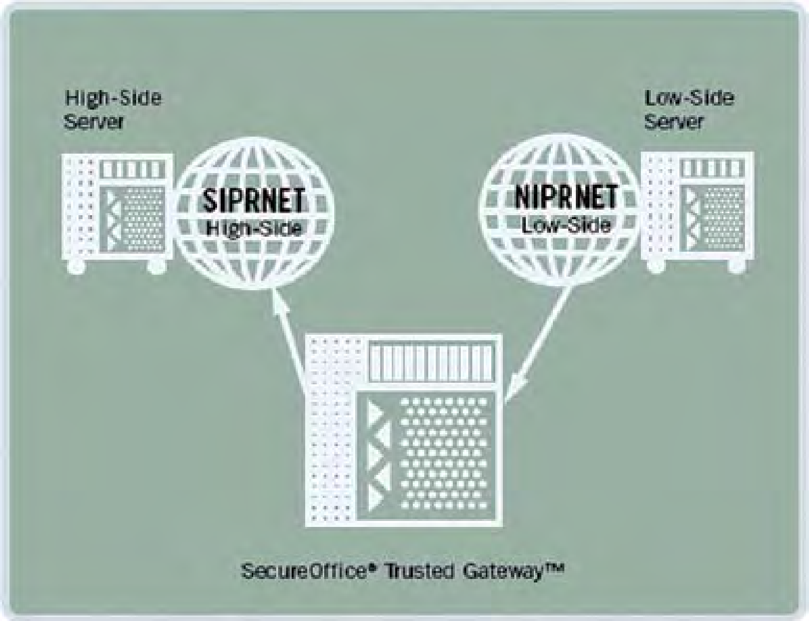
IT 1.05 UNABRIDGED ASSESSMENT LINK

Trusted Gateway System Guard

1. CROSS-DOMAIN DATA SHARING ●

TRIAL OVERVIEW: TGS Guard is a cross-domain solution offering secure one-way transfer of data from one network to another network of higher classification or sensitivity level. Using the TGS, an organization can electronically move large quantities of practically any type of data (e.g., imagery, maps, documents, e-mail, databases, etc.) from one network to another. TGS Guard facilitates data transfer in any format or from any operating system, UNIX or Microsoft and provides higher security, greater throughput, virus scanning, and file filtering.

SPONSOR:
US Air Force
LOCATIONS:
SPAWAR
ESC Hanscom
New Zealand
PARTNERS:
none



ASSESSMEMT RESULTS:
During CWID 2007, the TGS Trial operated on the CTF domain and received a Technical Interoperability assessment.

- TSG Guard successfully demonstrated CWID Objective 1 by executing secure one-way transfers of various types of imagery data from one network to another network of a higher classification or sensitivity level.

- TGS Guard successfully transferred text and JPEG files; other file types were blocked as 'dirty' files.

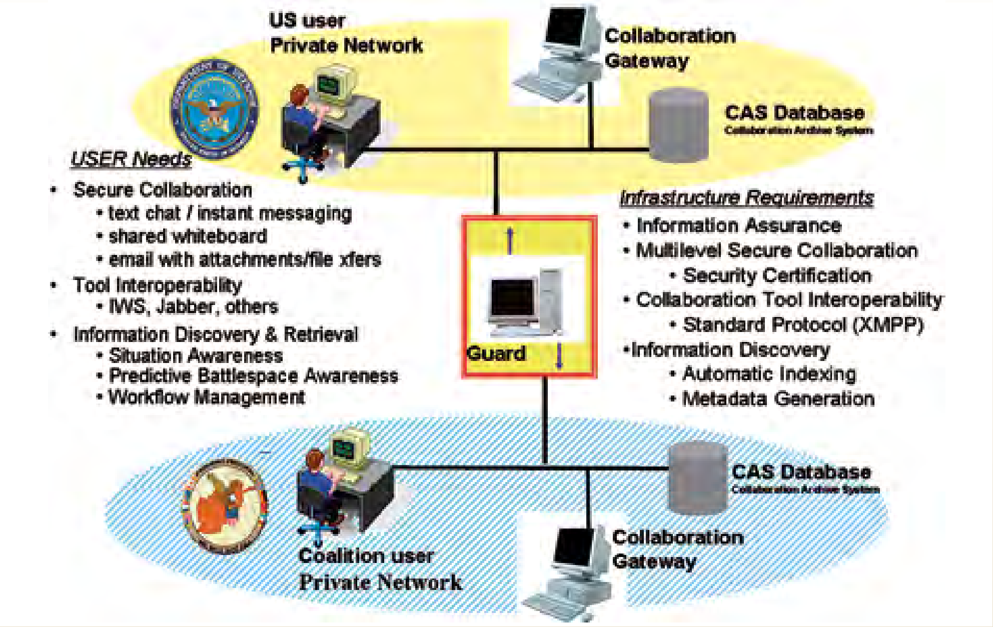
IT 1.17 UNABRIDGED ASSESSMENT LINK

Collaboration Gateway

1. CROSS-DOMAIN DATA SHARING● 3. NTEGRATED OPERATIONS ●

TRIAL OVERVIEW: Collaboration Gateway (CG), an umbrella program encompassing many Small Business Innovative Research (SBIR) initiatives, addresses the needs for Multi-level security (MLS) collaboration, interoperable collaboration tools, ISE discretionary access and information discovery. Collaboration Gateway (CG) is an open standards-based, turn-key system that enables secure cross-domain text chat, facilitates interoperability between different chat clients, and blocks chat messages that fail security checks. CG is integrated with certified guarding technology, and supports the standard eXtensible Messaging and Presence Protocol (XMPP) chat protocol.

SPONSOR:
USJFCOM
US Air Force
FBI
LOCATIONS:
USNORTHCOM
NSWC Dahlgren
SPAWAR
New Zealand
PARTNERS:
none



ASSESSMEMT RESULTS:
During CWID 2007, the CG Trial operated on the CTF and HS/HD domains and received a Warfighter, Technical Interoperability and a Targeted Information Assurance assessment.

■ CG successfully met CWID Objectives 1 and 3, providing users a secure cross-domain text chat capability using a Certified IISE Guard. Warfighters on HS/HD domain communicated using text chat with warfighters on the CTF domain demonstrating an integrated operations capability.

■ Warfighters using the CG IWS chat tool demonstrated chat room access denial capabilities due to improper credentials.

■ Trial did not demonstrate at USEUCOM and Canada due to minimal training, and insufficient technical support.

■ IA scans discovered correctable open ports and protocols, unneeded accounts and unnecessary services noted for correction in future releases.

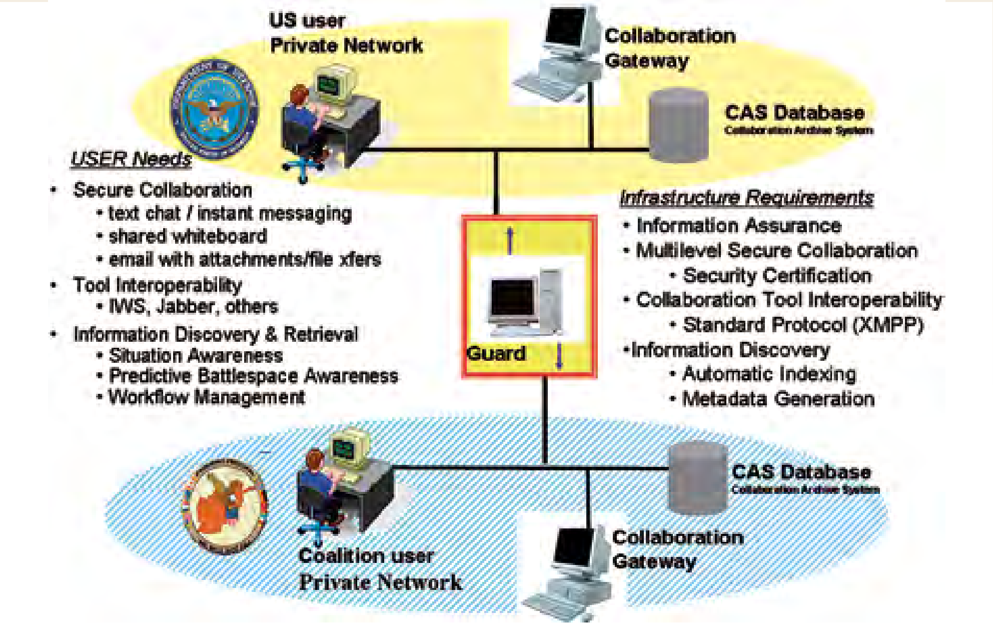
IT 1.17A UNABRIDGED ASSESSMENT LINK

Collaboration Gateway Collaboration Tools

1. CROSS-DOMAIN DATA SHARING ● 2. INTEGRATED INTELLIGENCE ● 3. INTEGRATED OPERATIONS ● 5. INTEGRATED PLANNING ●

TRIAL OVERVIEW: CGCT, an architectural design of an open standards-based, turn-key system, enables secure bi-directional cross-domain information sharing using a variety of collaboration tools. CGCT (v2.0) is an enhanced version of Collaboration Gateway v1.1, incorporating new intelligence analysis tools and function, including: Dolphin Star Guard with Desktop Dissemination Tool and Workflow enforcement Service, Chiliad Discovery/Alert and data mining with search functionality, Automated Course of Action Modeling, Peerless Service-based Product Automation and Dissemination Environment, and XpressRules.

SPONSOR:
USJFCOM
US Air Force
FBI
LOCATIONS:
USNORTHCOM
NSWC Dahlgren
SPAWAR
New Zealand
PARTNERS:
none**:**



ASSESSMENT RESULTS:
During CWID 2007, the CGCT Trial operated on the CTF and CTF High domain and received a SEIWG evaluation.

■ CGCT was partially successful meeting CWID objective 1 by demonstrating cross-domain chat with Collaboration Gateway v2.0 using the Transverse tool. Cross-domain data transfers were not demonstrated.

■ CGCT did not successfully meet CWID objectives 2, 3 and 5. While the CGCT Trial provides a promising comprehensive design of a cross-domain intelligence production tool set, it was too immature to bring to CWID 2007.

IT 1.28

UNABRIDGED ASSESSMENT LINK

NET/X eToken Security System, Deployable Communications System

2. INTEGRATED INTELLIGENCE ●

TRIAL OVERVIEW: NET/X is a USB platform that, when connected to any Intel/Windows based computer, converts the workstation or mobile device into a terminal. The NET/X device converts the existing network architecture to an integrated functional network, knocking down the "stovepipes" of information access, then back to its original state when disconnected. The NET/X token also allows users to connect to any workstation with internet connectivity anywhere, providing a secure terminal "tunnel" reaching back to IT Centers. In its most common mode of operation, the user (at laptop) is in a "read only" mode for data/graphics/text on the server.

SPONSOR:
USJFCOM
LOCATIONS:
USNORTHCOM
NSWC Dahlgren
SPAWAR
PARTNERS:
none

ASSESSMEMT RESULTS:
During CWID 2007, the NET/X Trial operated on the HS/HD domain and received a Basic Information Assurance (IA) assessment and a SEIWG evaluation.

- NET/X successfully met CWID Objective 2 by providing on-the-move warfighters with access to secure, up-to-date information resources while in transit by dynamically creating secure network tunnels that reached back to IT Centers.
- Successfully validated security requirements leaving no residual data on remote workstations when disconnected from NET/X eToken.
- Successfully demonstrated immediate access to secure net-centric data with real-time data stores.
- No IA vulnerabilities found.

IT 1.43

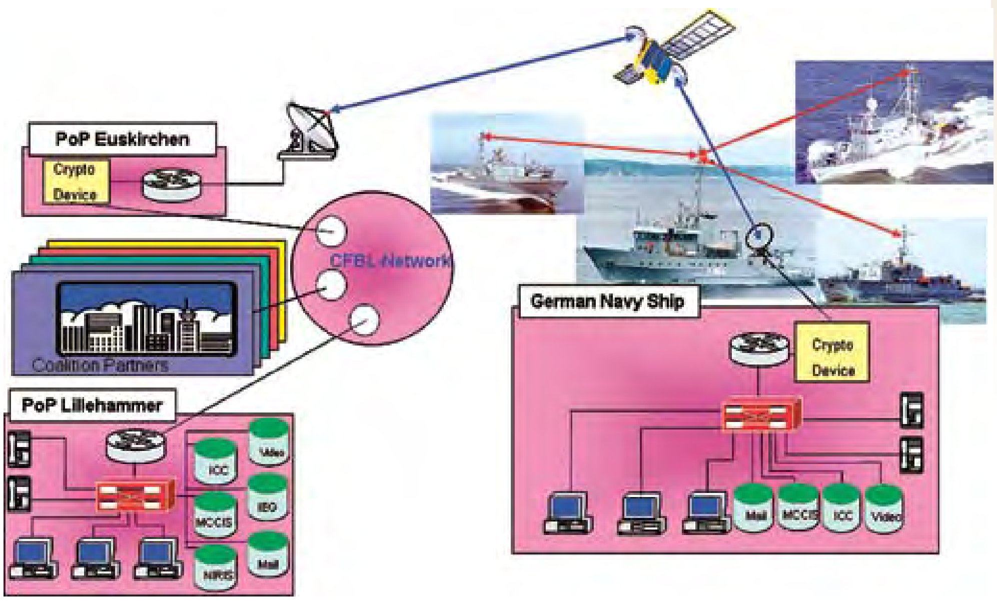
UNABRIDGED ASSESSMENT LINK

Mobile Forces Solution-Subnet Relay

1. CROSS-DOMAIN DATA SHARING ●

TRIAL OVERVIEW: The MOFS-SNR is a distributed Internet Protocol (IP) infrastructure with secure broadband satellite communication to ships and secure Subnet Relay via HF/UHF and DVB-T that provides data exchange amongst multiple applications such as MCCIS, ICC, email, ERP-System, VoIP and Video Conference. MOFS-SNR also provides Maritime, Air and Joint C2 services to include secure communications redundancy for ships with satellite links, connectivity for disadvantaged ships without satellite access, and facilitates a complete accurate and on-time operational picture.

SPONSOR:
Germany
LOCATIONS:
SPAWAR
NATO
PARTNERS:
none



ASSESSMEMT RESULTS:
During CWID 2007, the MOFS-SNR Trial operated on the CTF domain and received a Warfighter assessment and a SEIWG evaluation.

- MOFS successfully created a subnet relay for a secure communications path between deployed units without satellite access and units with satellite access to share data in multiple formats.
- MOFS was moderately successful facilitating battle planning and information dissemination because bandwidth issues contributed to less than 100% reliability as evidenced by unstable connectivity and problematic video teleconferencing.

IT 1.54

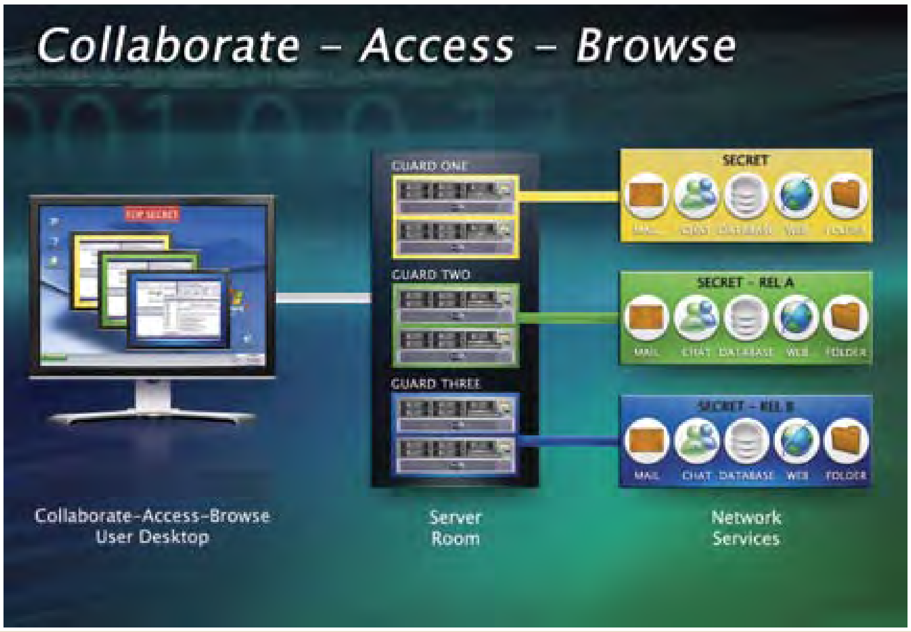
UNABRIDGED ASSESSMENT LINK

Collaborate-Access-Browse

1. CROSS-DOMAIN DATA SHARING ●

TRIAL OVERVIEW: CAB is a secure desktop reduction solution that allows users on a higher security network to have full access to applications and files resident on a lower security network from their existing high side workstation. Using a guard and a lightweight Java application, rapid deployment of a new network or quick access to an existing network is possible. CAB blocks transfer of classified information from the high to the low-side network, is supported by Windows 2000 or newer, and requires only 1/2 rack of server room hardware. CAB supports lower domain web browsing, e-mail, Office applications, databases, etc., and supports up to 200 users on a single guard.

SPONSOR:
USJFCOM
LOCATIONS:
USEUCOM
USNORTHCOM
NSWC Dahlgren
SPAWAR
ESC Hanscom
New Zealand
PARTNERS:
none



ASSESSMEMT RESULTS:
During CWID 2007, the CAB Trial operated on the CTF and CTF High domains and received a Technical Interoperability assessment.

- CAB successfully met CWID Objective 1. Warfighters used the CAB web-based interface to access a lower security domain (CTF) from a high side desktop (CTF-High). After accessing the low side workstation, warfighters successfully accessed and manipulated multiple document types and images (MSWord, PowerPoint, Excel spreadsheets, JPEG and Gif).

- Successfully demonstrated email and chat functions to include a dirty word filter capability.

IT 1.55

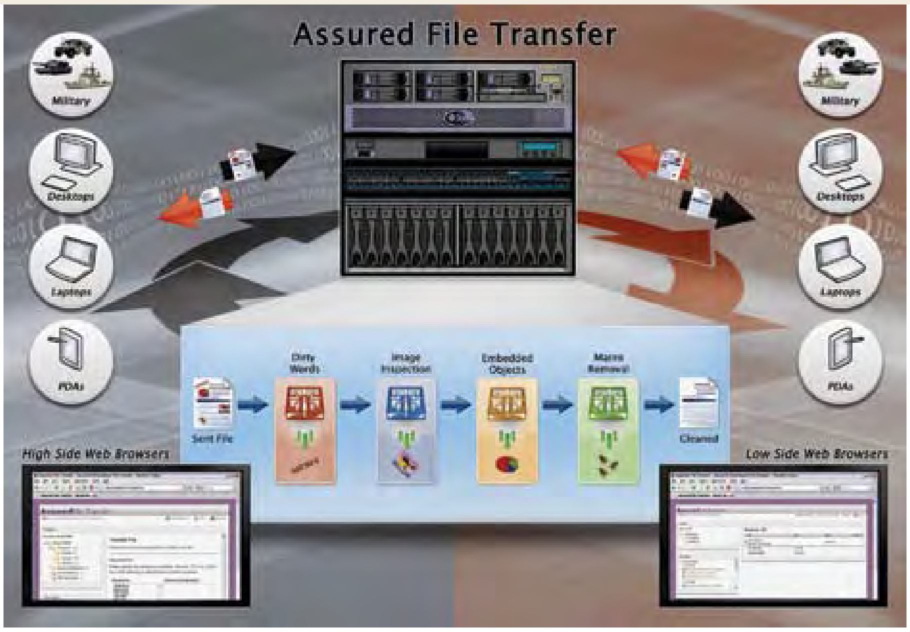
UNABRIDGED ASSESSMENT LINK

Assured File Transfer

1. CROSS-DOMAIN DATA SHARING ●

TRIAL OVERVIEW: AFT securely transfers high-risk complex files bi-directionally between domains of varying security classifications. AFT cleans files by removing malicious, hidden, and inappropriate content before sending.
AFT transfers files without revealing sensitive information while retaining native formats, has no impact on client machines, and can be used as a policy enforcement tool and a desk-top cleaning tool for High-Side users. AFT provides machine-to-machine capability and interoperates with any high-side workstation supporting a modern browser.

SPONSOR:
NSA
LOCATIONS:
USEUCOM
USNORTHCOM
NSWC Dahlgren
SPAWAR
ESC Hanscom
New Zealand
PARTNERS:
none



ASSESSMEMT RESULTS:
During CWID 2007, the AFT Trial operated on the CTF and CTF High domains and received Warfighter, Technical Interoperability, and Targeted Information Assurance assessments.

- AFT successfully met CWID Objective 1 by allowing secure bi-directional transfer of multiple file types between the CTF and CTF High domains, simulating a cross-domain environment. The foreign disclosure officer (FDO) approved file content before transfer to a lower security domain. Files retained the original file format.

- AFT allowed seamless and quick file sharing between security domains, improving situational awareness, threat assessment, and decision-making timelines.

- No IA vulnerabilities found.

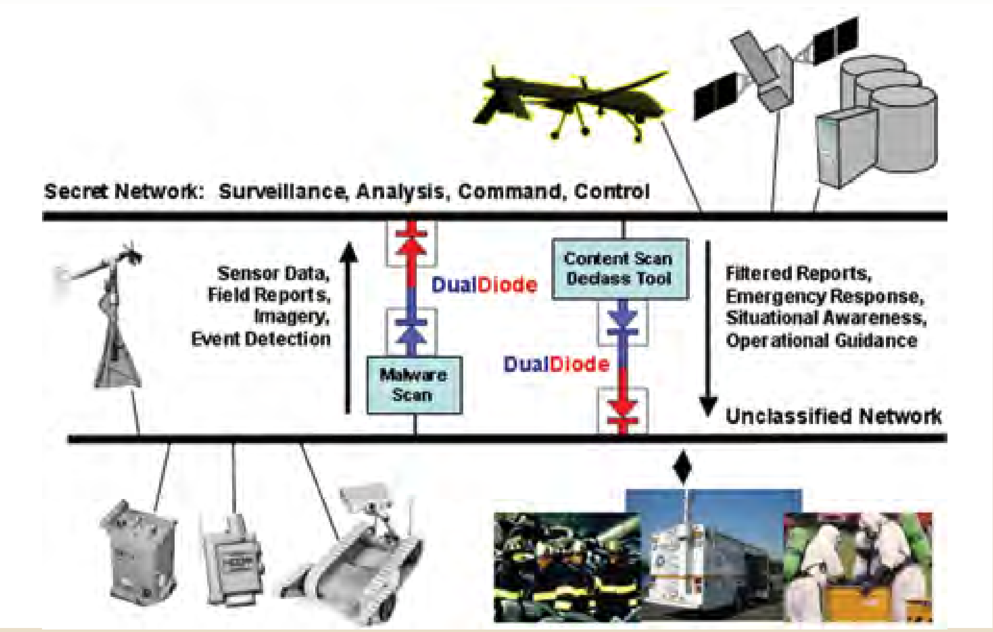
IT 1.56 UNABRIDGED ASSESSMENT LINK

Dual Diode Secure (One-Way) Cross-Domain Data Transfer System

1. CROSS-DOMAIN DATA SHARING ●

TRIAL OVERVIEW: The Dual Diode provides a one-way real-time data link between isolated network security domains that are certified, accredited, and deployed throughout DoD and the U.S. intelligence community. Dual Diode consists of a pair of custom fiber optic network interface cards (send-only and receive-only) installed in host computer platforms on separate networks. Hardware enforces high forward data flow (155 Mbps) and denies backward data flow. For CWID, Dual Diode integrated content scanning software to provide cross-domain data transfer solutions in up guard, peer guard and down guard configurations. Content scanning included anti-malware for up guards and human review and declass tools for down guards.

SPONSOR:
Canada
LOCATIONS:
SPAWAR
Canada
New Zealand
PARTNERS:
IT 3.27


Secret Network: Surveillance, Analysis, Command, Control
Sensor Data, Field Reports, Imagery, Event Detection
DualDiode
Content Scan Declass Tool
Filtered Reports, Emergency Response, Situational Awareness, Operational Guidance
Malware Scan
DualDiode
Unclassified Network

ASSESSMEMT RESULTS:
The Dual Diode Trial operated on the HS/HD, CTF and CTF High domains, receiving Warfighter and Technical Interoperability assessments.

- Owl Dual Diode successfully met CWID Objective 1, enhancing coalition information sharing capabilities among allies and coalition partners, by enabling file transfer and streaming video across different security domains. Owl demonstrated transfer up and down network security classifications (i.e. from HS to CTF, from CTF High to CTF, from HS to a simulated unclassified).
- Owl successfully passed text files (.txt, .csv, .htm, .rtf), Microsoft office files, Adobe PDF, Image files (JPEG, GIF, BMP, CADRG, DTED, Vmap, CIB, TIFF), and entire file directories. Owl successfully used SharePoint to send and receive.
- Warfighters found Owl quick, easy to use, reliable, and with some updates, ready to deploy.
- Owl successfully demonstrated "dirty word" file searches.

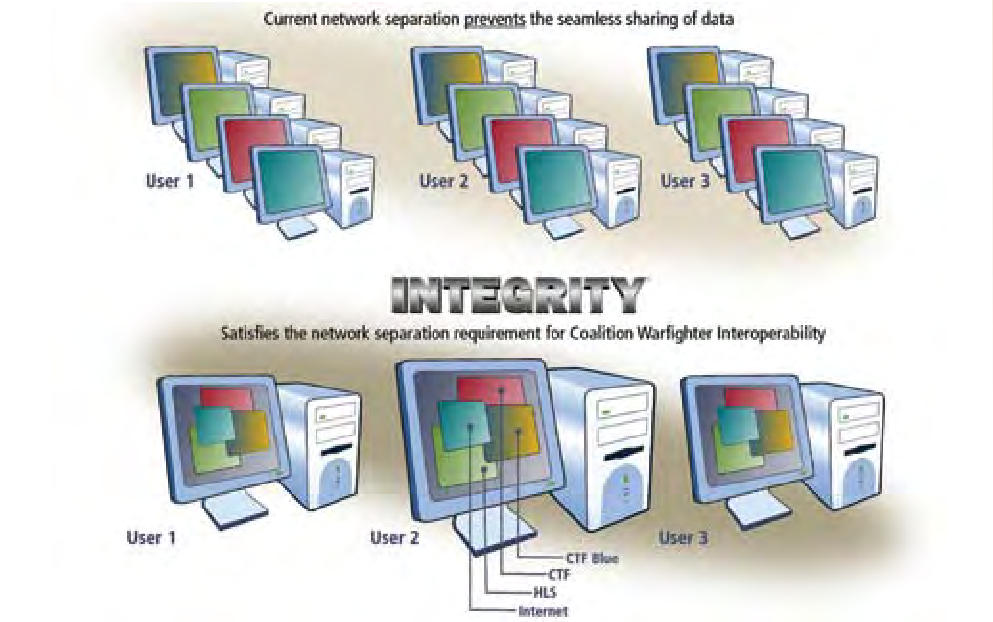
IT 1.61 UNABRIDGED ASSESSMENT LINK

INTEGRITY Secure Workstation

1. CROSS-DOMAIN DATA SHARING ●

TRIAL OVERVIEW: INTSecWS provides information sharing across multiple networks of potentially different security classifications and caveats as well as improves information sharing by using secure operating systems and applications to facilitate battle planning and information dissemination. INTSecWS extends the safety and security attributes of a weapons system to the desktop while ensuring Windows and Linux applications are isolated, protected, and guaranteed. INTSecWS is recognized as the only capabilities-based microkernel that can provide guaranteed resource availability.

SPONSOR:
Canada
LOCATIONS:
Canada
PARTNERS:
none


Current network separation prevents the seamless sharing of data
User 1
User 2
User 3
INTEGRITY
Satisfies the network separation requirement for Coalition Warfighter Interoperability
User 1
User 2
User 3
CTF Blue
CTF
HLS
Internet

ASSESSMENT RESULTS:
During CWID 2007, the INTSecWS Trial operated on the CTF and CTF High domains and received a Technical Interoperability assessment.

- INTSecWS successfully met CWID Objective 1. INTSecWS allowed seamless viewing and secure transfer of information among different security levels. The system successfully facilitated three classification domains on a single workstation (i.e. CTF High, CTF, and a simulated unclassified).
- Warfighters agreed INTSecWS worked well, was easy to use, stable, reliable, and helped them accomplish their tasks. Warfighters were impressed with the technology and supported deployment in its current configuration.

IT 1.63

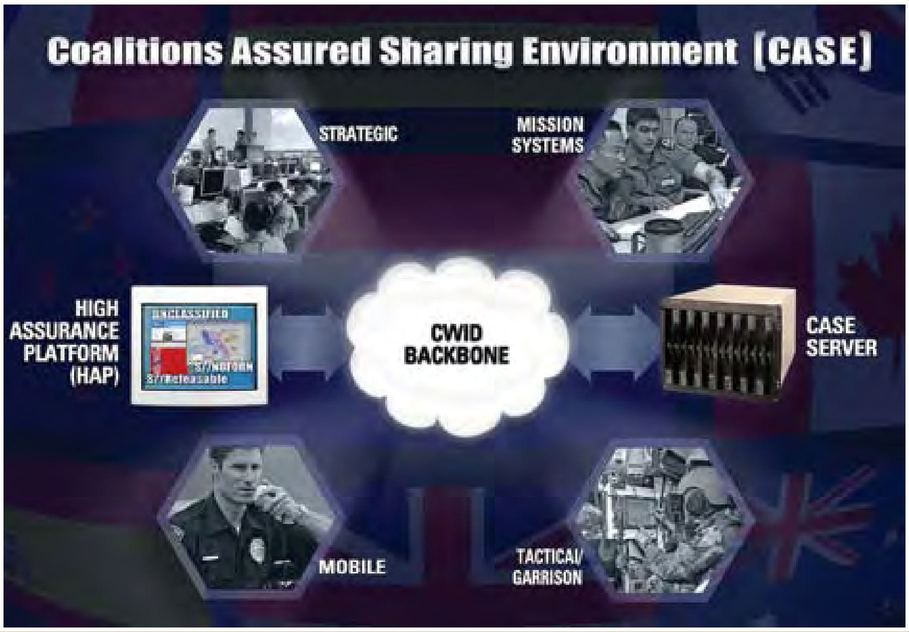
UNABRIDGED ASSESSMENT LINK

Coalition Assured Sharing Environment

2. INTEGRATED INTELLIGENCE ●

TRIAL OVERVIEW: GD CASE provides an enterprise solution to use information from different Communities of Interest (COIs) and security domains on a single High Assurance Platform (HAP), accesses information and enterprise applications based on COI membership, and moves information between security domains via an integrated, certified and accredited cross-domain guard and workflow toolset. CASE's COI separation technology uses Type 2 VPNs to provide secure, separated flows across a common network backbone. In addition, each data transaction is labeled for assessment by a dynamic policy engine for real-time enforcement based on dynamic policies.

SPONSOR:
DISA
LOCATIONS:
USNORTHCOM
NSWC Dahlgren
PARTNERS:
none



ASSESSMEMT RESULTS:
GD CASE operated on the CTF and HS/HD domains, receiving Warfighter, Technical Interoperability, and Targeted Information Assurance (IA) assessments.

- GD CASE successfully met CWID Objective 2 by allowing simultaneously log in and navigation between disparate domains using a unique Virtual Private Network (VPN) based on token CAC (Common Access Card) log in. This feature allowed concurrent information review from multiple inputs on the same workstation.
- GD CASE provided downgrade or upgrade data for users to efficiently share time-sensitive data while protecting data.
- GD CASE allowed concurrent establishment of different COIs, development of unique "need-to-know" rules, and ability to change rules as situations warranted.
- IA scans discovered correctable open ports and protocols, unneeded accounts and unnecessary services noted for correction in future releases.

IT 1.86

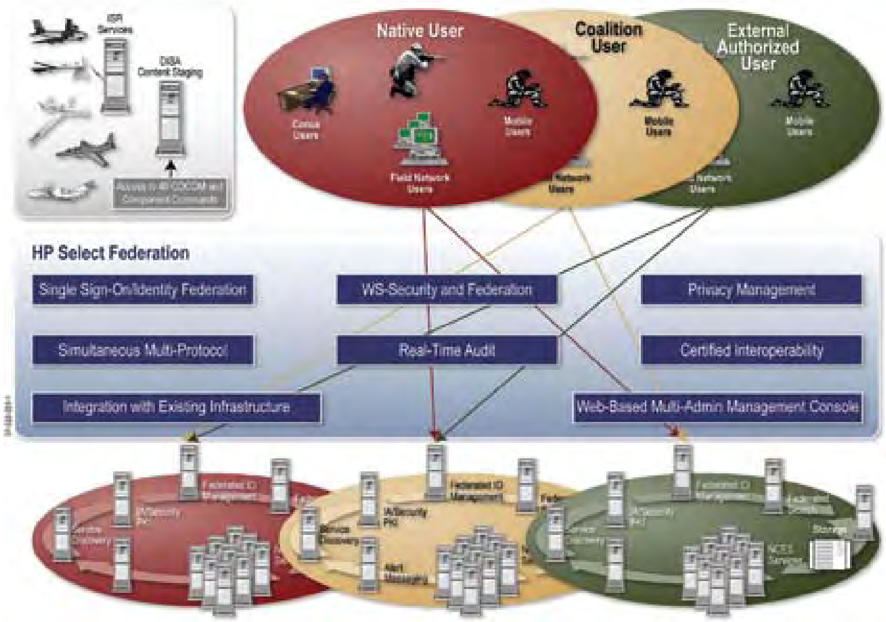
UNABRIDGED ASSESSMENT LINK

Federated Identity Management System

1. CROSS-DOMAIN DATA SHARING ●

TRIAL OVERVIEW: FIDMS is a robust federated identity management service, designed to ensure authorized users in multiple security domains have access to all appropriate resources within their home security domain and remote security domains while preserving the integrity of security policies established for each domain. FIDMS is a COTS-based solution that provides integrated identity validation and verification to users across distributed security domain and sites without having to replicate their identities in each domain. FIDMS's infrastructure provides a superior online experience, personalization, security and control over identity information.

SPONSOR:
USJFCOM
LOCATIONS:
USNORTHCOM
NSWC Dahlgren
Hanscom
PARTNERS:
none



ASSESSMENT RESULTS:
During CWID 2007, the FIDMS Trial operated on the CTF and HS/HD domains and received Technical Interoperability and Basic Information Assurance (IA) assessments.

- FIDMS successfully met CWID Objective 1 by authenticating and connecting users to information resources in differing security domains within the HS/HD and CTF enclaves without replicating identities.
- Through its federated page, FIDMS authenticated users who could only access information resources located at Dahlgren through an established link.
- IA scans discovered correctable open ports and protocols, unneeded accounts and unnecessary services noted for correction in future releases.

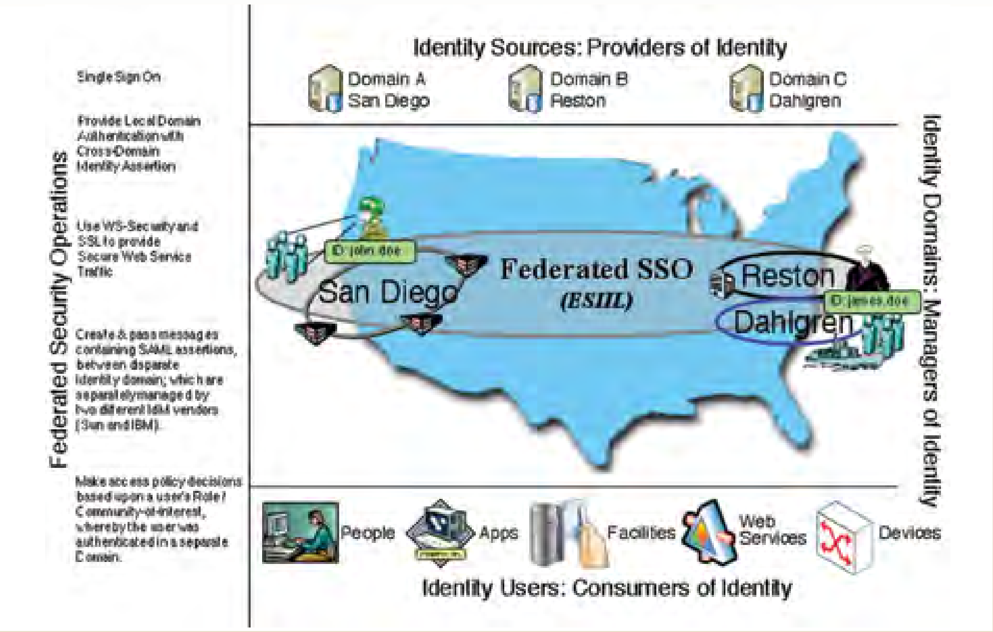
IT 1.87 UNABRIDGED ASSESSMENT LINK

Federated Security

1. CROSS-DOMAIN DATA SHARING ●

TRIAL OVERVIEW: FS performs cross-domain identity management and single sign-on using COTS identity management products in a Service Oriented Architecture (SOA) environment, a DoD and DHS challenge because of the multitude of different networks that exist at the federal, state, and local level. FS removes the need for distributed user account provisioning and simplifies new development by shifting common security functions out of the application and into the middleware. Security is based on pre-established lines of trust between domains as well as digitally signed authorization credentials. FS enhances information sharing across different organization at the local, state, and federal level by providing centralized policy management and enforcement.

SPONSOR:
USJFCOM
LOCATION:
NSWC Dahlgren
PARTNERS:
none


Federated Security Operations
Single Sign On
Provide Local Domain Authentication with Cross-Domain Identity Assertion
Use WS-Security and SSL to provide Secure Web Service Traffic
Create & pass messages containing SAML assertions, between disparate identity domain; which are separately managed by two different IdM vendors (Sun and IBM).
Make access policy decisions based upon a user's Role / Community-of-interest, whereby the user was authenticated in a separate Domain.
Identity Sources: Providers of Identity
Domain A San Diego
Domain B Reston
Domain C Dahlgren
Federated SSO
(ESIIL)
San Diego
Reston
Dahlgren
ID: john.doe
ID: james.doe
Identity Domains: Managers of Identity
People
Apps
Facilities
Web Services
Devices
Identity Users: Consumers of Identity

ASSESSMEMT RESULTS:
The FS Trial operated on the HS/HD domain, receiving Technical Interoperability and Basic Information Assurance (IA) assessments.

- FS successfully met CWID Objective 1 by demonstrating cross-domain authorization using SAML (Security Assertion Markup Language) for user data access.
- Using a specified URL, users gained access to the FS project as a single sign-on user granted appropriate access to applications. For example, user in COI 'A' accessed information and resources in a trusted COI 'B' without the need to manage the user's identity in both domains.
- FS successfully encrypted and transferred data, including NGA imagery, via a mutual SSL connection between domains.
- IA scans discovered correctable open ports and protocols, unneeded accounts and unnecessary services noted for correction in future releases.

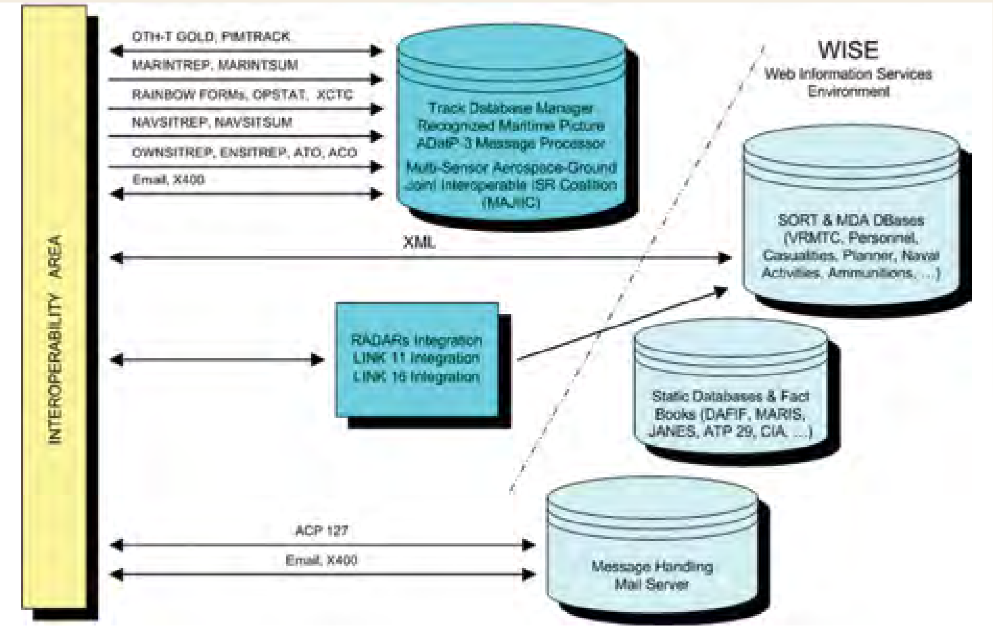
IT 2.06 UNABRIDGED ASSESSMENT LINK

Italian Navy Maritime Command & Control Information System

2. INTEGRATED INTELLIGENCE ●

TRIAL OVERVIEW: MCCIS-Italy v.5.2 was developed and maintained to allow maritime commanders and staffs to automatically acquire and maintain large quantities of information for display and analysis. The trial electronically processes multiple source data, displays the information in various Command and Control (C2) applications and provides users with the ability to manipulate the data to assist strategic, operational and tactical commanders (and staffs) in decision making processes. MCCIS-Italy v.5.2 provides RMP, MTF, SORT, MDA data and e-mail exchange, testing the capability of the new release to be fully interoperable and integrate with other US CWID 2007 C4I systems.

SPONSOR:
Italy
LOCATIONS:
SPAWAR
NATO
PARTNERS:
none


INTEROPERABILITY AREA
OTH-T GOLD, PIMTRACK
MARINTREP, MARINTSUM
RAINBOW FORMs, OPSTAT, XCTC
NAVSITREP, NAVSITSUM
OWNSITREP, ENSITREP, ATO, ACO
Email, X400
Track Database Manager
Recognized Maritime Picture
ADatP 3 Message Processor
Multi-Sensor Aerospace-Ground Joint Interoperable ISR Coalition (MAJIIC)
XML
WISE
Web Information Services Environment
SORT & MDA DBases (VRMTC, Personnel, Casualties, Planner, Naval Activities, Ammunitions, ...)
RADARs Integration
LINK 11 Integration
LINK 16 Integration
Static Databases & Fact Books (DAFIF, MARIS, JANES, ATP 29, CIA, ...)
ACP 127
Email, X400
Message Handing Mail Server

ASSESSMENT RESULTS:
The MCCIS-Italy Trial operated on the CTF domain, receiving Warfighter and Technical Interoperability assessments.

- MCCIS successfully met CWID Objective 2 by exchanging and correctly displaying track data, with the exception of air track data, between the U.S. GCCS-J and GCCS-M systems, providing an enhanced COP through intelligent retrieval and data fusion from disparate sources.
- MCCIS successfully received, processed, and displayed OTH-Gold messages from GCCS-J/M systems. MCCIS sent OTH-Gold messages to GCCS-J/M, where they were also processed and displayed correctly.
- MCCIS could not process and display ATO messages, formatted as either USMTF or ADatP-3, sent from GCCS-J.
- Operators tested a new web-based portal functionality allowing authorized users to access data from various sources without MCCIS software.

IT 2.16

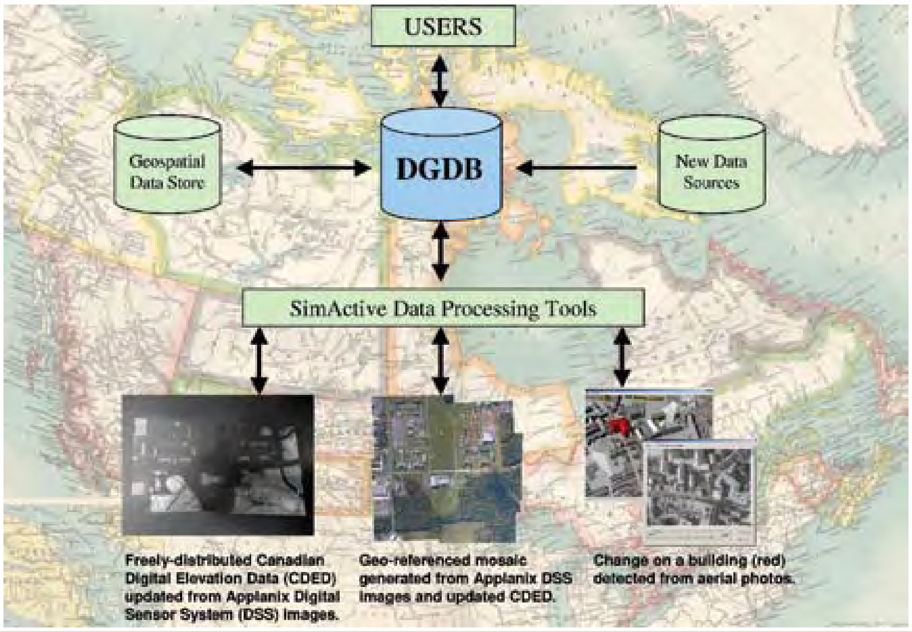
UNABRIDGED ASSESSMENT LINK

Deployable Geospatial Database

2. INTEGRATED INTELLIGENCE ●

TRIAL OVERVIEW: DGDB, a data model to support mission-specific in-theater operations, is a new approach developed under ArcSDE (Shared Data Environment) to manage, share and disseminate data at theater-wide level. This model is based on the U.S. Theatre Geospatial Database (TGD). DGDB also integrates SimActive technology, developed in collaboration with DRDC Valcartier, Canada. DGDB allows automatic integration of 2-D imagery, such as aerial photos, with 3-D data (e.g. Digital Elevation Models) and can register imagery with 3-D data for the creation of precise ortho-photos. DGDB also detects 3-D differences and updates 3-D data to track structural changes or improve the quality of an existing 3-D data set.

SPONSOR:
Canada
LOCATIONS:
Canada
PARTNERS:
none



Freely-distributed Canadian Digital Elevation Data (CDED) updated from Applanix Digital Sensor System (DSS) images.

Geo-referenced mosaic generated from Applanix DSS images and updated CDED.

Change on a building (red) detected from aerial photos.

ASSESSMEMT RESULTS:
The DGDB Trial operated on the HS/HD domain, receiving a Warfighter assessment.

- DGDB successfully met CWID Objective 2 of enhancing coalition information and knowledge sharing capabilities by enabling the collection of all available data for a specified area so that all the basic required data was deployed with the geomatics technician.
- DGDB successfully provided the ability to update and improve the resolution of a 3D elevation model by using high-resolution imagery.
- Warfighters found that DGDB worked well and was very reliable. They found the system more or less easy to use, quoting data structure issues as the main drawback. The SimActive tool to update elevation data and to generate ortho-rectified, geo-referenced mosaic images was very fast and easy.
- Warfighters supported deployment with an improved data/file structure.

IT 2.21

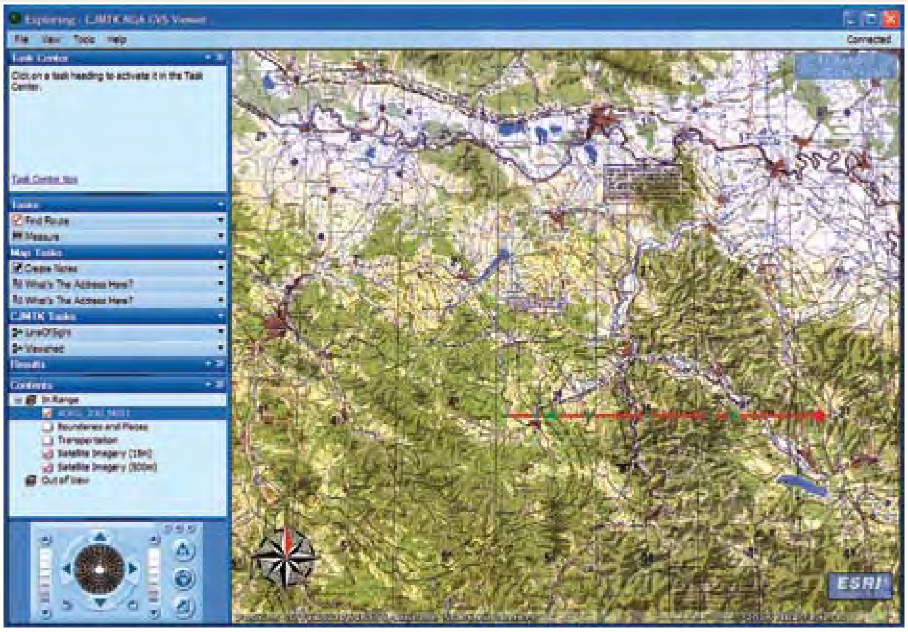
UNABRIDGED ASSESSMENT LINK

Commercial Joint Mapping Toolkit

2. INTEGRATED INTELLIGENCE ●

TRIAL OVERVIEW: CJMTK is the recommended geospatial software toolkit for the DoD Command and Control Intelligence (C2I) community to perform situational analysis such as determining troop locations or identifying the most efficient routes for moving troops and equipment. In addition, CJMTK provides map data in an application-ready format, allowing systems to see and use map data without software compatibility issues. CJMTK capabilities employ the Web which allows other client systems to use the systems tools for conducting analysis and viewing data.

SPONSOR:
NGA
LOCATIONS:
USNORTHCOM
NSWC Dahlgren
SPAWAR
ESC Hanscom
United Kingdom
PARTNERS:
none



Click on a task heading to activate it in the Task Center.

ASSESSMENT RESULTS:
The CJMTK Trial operated on the CTF domain and received Warfighter, Technical Interoperability and Basic Information Assurance (IA) assessments.

- CJMTK successfully met CWID Objective 2 through the effective use of line-of-site analysis, movement projection analysis, and viewshed analysis, providing commanders an improved intelligence information sharing capability.
- Graphics generated using CJMTK tools were successfully saved as JPEG files and shared with users that did not have access to the CJMTK system. These JPEG files provided commanders with up-to-the minute, real-time graphical situational awareness.
- Warfighters successfully created and shared detailed annotated maps with coalition partners and other agencies.
- IA scans found some open ports and protocols.

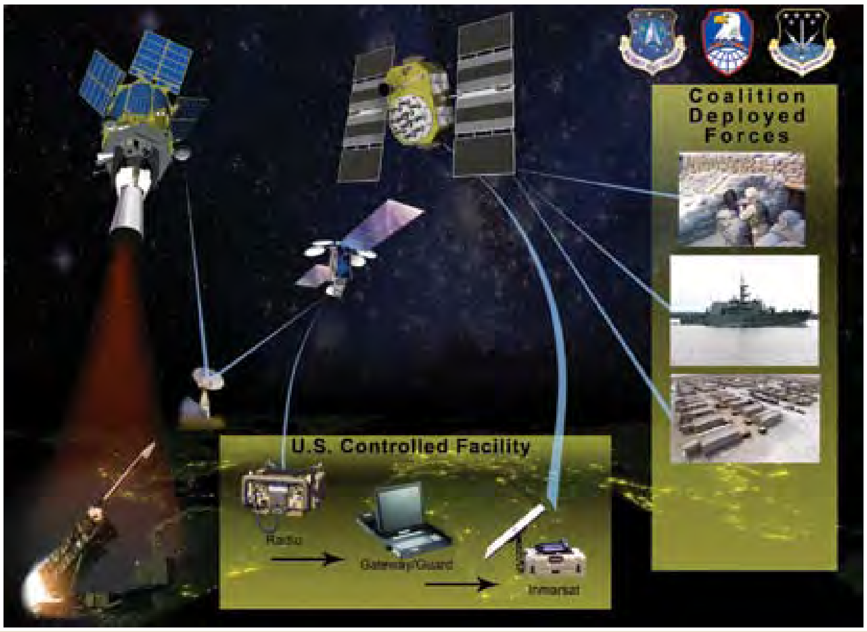
IT 2.37 UNABRIDGED ASSESSMENT LINK

Rapid Force Warning

1. CROSS-DOMAIN DATA SHARING ● 2. INTEGRATED INTELLIGENCE ● 3. INTEGRATED OPERATIONS ●

TRIAL OVERVIEW: RFW provides the ability to rapidly deploy, setup, and configure missile early warning capabilities in support of operations at immature or austere sites: sites where communication infrastructures or permanent facilities are not established. RFW enables the sharing of missile warning data with coalition forces and has the unique ability to tailor reporting of ballistic missile threats in the region utilizing a rule-based gateway. RFW offers commanders a tool to rapidly establish sharing of missile warning data releasable to coalition forces. RFW utilizes a pay-by-the-packet methodology—paying only for data processed while maintaining a small footprint. This rapidly deployable and low cost capability can enhance passive or active defense, attack operations and battle space situational awareness.

SPONSOR:
US Air Force
LOCATIONS:
ESC Hanscom
NATO
PARTNERS:
IT 3.31



ASSESSMEMT RESULTS:
During CWID 2007, the RFW Trial operated on the CTF domain and received a Technical Interoperability assessment.

■ RFW successfully met CWID Objectives 1, 2, and 3 by disseminating releasable Missile Warning (MW) data to US and NATO GCCS systems.

■ Using a NSA approved secure guard, RFW successfully declassified track data and automatically disseminated the data to a standalone GCCS laptop at Hanscom where an audible alert was produced. Users viewed the declassified data on the GCCS laptop map.

■ RFW shared downgraded missile warning data with NATO, via INMARSAT, rapidly enhancing situational awareness for the area of operations.

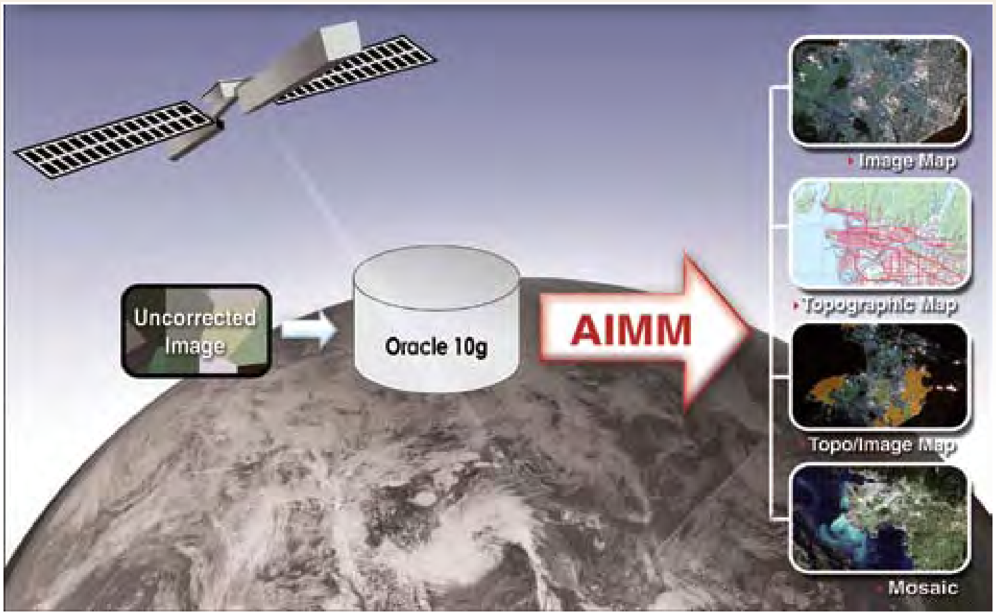
IT 2.57 UNABRIDGED ASSESSMENT LINK

Automatic Ingest Mosaic Mapping System

2. INTEGRATED INTELLIGENCE ●

TRIAL OVERVIEW: AIMM is a cost-effective and time-efficient system for transforming geospatial data and imagery into critical decision support information. An automated production environment, AIMM ingests a wide variety of satellite imagery, automatically determines the satellite type, corrects the raw imagery to remove distortions, and inserts this imagery into an Oracle 10g database. Operators query available imagery for their area of interest via a web interface, based on any or all of the following options: location, time of acquisition, resolution, and sensor type. The system automatically responds and sends the requested imagery via FTP or email. AIMM offers a vast variety of possible output formats (e.g. a geocoded image in NITF format, GeoTiff, JPEG, a multiple image mosaic product, or a finished map product).

SPONSOR:
Canada
LOCATIONS:
USNORTHCOM
NSWC Dahlgren
SPAWAR
Canada
PARTNERS:
none



ASSESSMENT RESULTS:
The AIMM Trial operated on the CTF and HS/HD domains, receiving a Warfighter assessment and a SEIWG evaluation.

■ AIMM successfully met CWID Objective 2 of enhancing coalition information and knowledge sharing capabilities among allies and coalition partners by enabling the automatic generation of geomatic image mosaics for a specified area of interest and by ingesting and ortho-rectifying raw satellite imagery.

■ AIMM's maps exceeded the standard, though some warfighters found the quality inconsistent and the response time slow and felt that modifications to elements such as the AOI interface is necessary before deployment. Others were impressed with the product as demonstrated at CWID.

■ Successfully demonstrated operations between Department of Homeland Security (DHS) and Public Safety and Emergency Preparedness Canada (PSEPC).

IT 2.88

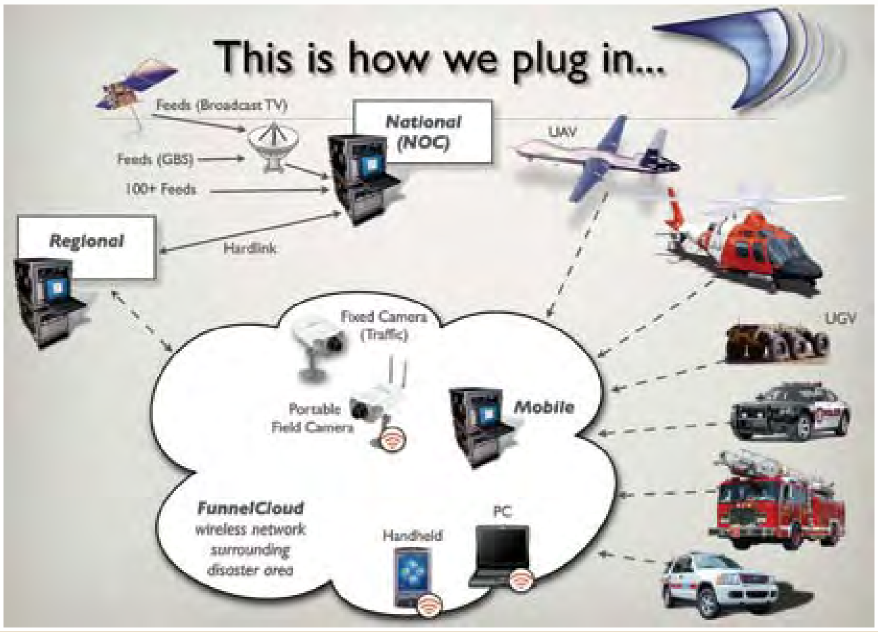
UNABRIDGED ASSESSMENT LINK

AdLib

2. INTEGRATED INTELLIGENCE ●

TRIAL OVERVIEW: AdLib captures and stores (60-to-90-days) analog and/or digital video and metadata, enabling intelligent location, access/control, and alerting of fixed and mobile video sources such as Unmanned Aerial Vehicles (UAVs). As a Web Services solution, AdLib integrates into video data and sensor feeds from multiple collection platforms, mobile/portable video sources, and sensor data capture sources. AdLib integrated Falconview, ESRI, Google Earth, Cursor on Target, C2PC and Federated Search NCES applications. It encrypts and compresses video/sensor data feeds, and applies Transport Layer Security (TLS) to redistribute context-specific video/sensor feeds using various computer/communication devices over low bandwidth in 18 seconds.

SPONSOR:
USNORTHCOM
LOCATIONS:
NSWC Dahlgren
United Kingdom
PARTNERS:
none



ASSESSMENT RESULTS:
AdLib operated on the HS/HD domain, receiving a Targeted Information Assurance (IA) assessment and a SEIWG evaluation.

■ Successfully met CWID Objective 2 by demonstrating a mobile, comprehensive tactical data collection system for C4ISR activities supporting warfighters and tactical command posts.

■ AdLib successfully demonstrated setting-up and controlling sensitivity levels of surveillance equipment (i.e. cameras) around a mobile unit to provide feedback for objects of interest. This system concept revolutionizes a tactical requirement for perimeter defense.

■ Successfully demonstrated collection of Buster UAV data for the mobile unit and forwarded data to decision-makers and warfighters.

■ IA scans discovered correctable open ports and protocols, unneeded accounts and unnecessary services noted for correction in future releases.

IT 3.09

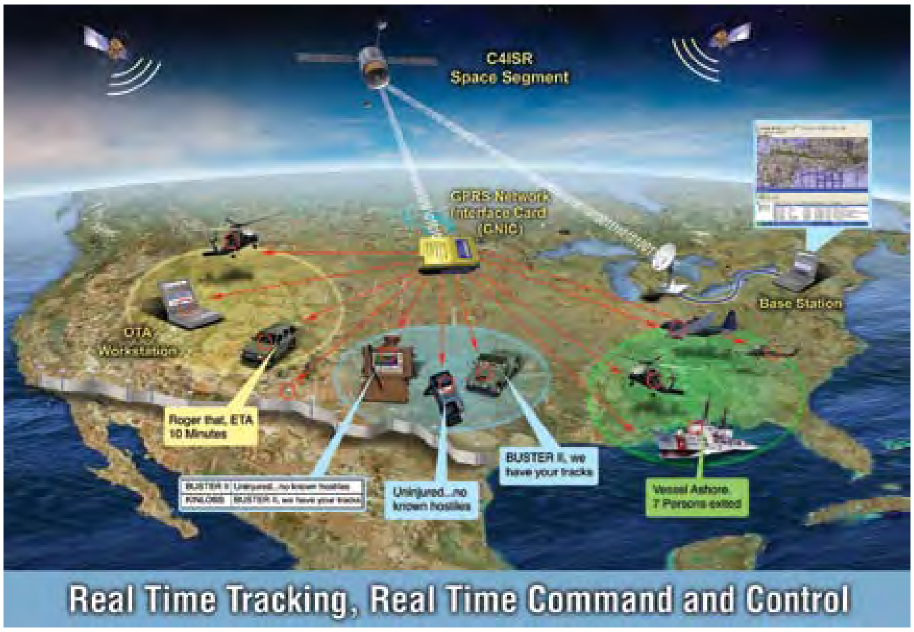
UNABRIDGED ASSESSMENT LINK

Global Personnel Recovery System

1. CROSS-DOMAIN DATA SHARING ● 2. INTEGRATED INTELLIGENCE ● 3. INTEGRATED OPERATIONS ● 4. INTEGRATED LOGISTICS ● 5. INTEGRATED PLANNING ●

TRIAL OVERVIEW: GPRS, a two-way messaging and tracking system, links mobile and fixed surface and airborne users and command/control elements at any distance and provides flexible, nearly instantaneous communications and locations via satellite. It rapidly groups and regroups response teams to meet changing needs. GPRS allows DoD and civilian search and rescue personnel to quickly identify and accurately locate people in need of rescue services anytime, anywhere in the world. GPRS enhances responsiveness across civil and other government organizations, providing aircraft and vehicle tracking, remote sensing, and command and control of rescue and first responder organizations.

SPONSOR:
USJFCOM
LOCATIONS:
USEUCOM
USNORTHCOM
NSWC Dahlgren
PARTNERS:
none


C4ISR Space Segment
GPRS Network Interface Card (GNIC)
Base Station
OTA Workstation
Roger that, ETA 10 Minutes
BUSTER II | Uninjured...no known hostiles
KINLOSS | BUSTER II, we have your tracks
Uninjured...no known hostiles
BUSTER II, we have your tracks
Vessel Ashore. 7 Persons exited
Real Time Tracking, Real Time Command and Control

ASSESSMENT RESULTS:
GPRS operated on the CTF and HS/HD domains, receiving Warfighter, Technical Interoperability and Basic Information Assurance (IA) assessments.

■ GPRS successfully met CWID Objectives 1, 2, 3, 4, and 5 by providing real-time tracking of remote troop locations, converting data to USMTF format and forwarding for display on CTF GCCS COP and HD COP.

■ GPRS information was verified as accurate and pertinent to users. However, warfighters reported some problems ensuring devices were pointed to the southern sky in order to have 2-way communication.

■ Additionally, GPRS participated at the following locations using operational warfighters: Hulbert Field, Eglan Air Force Base, FL, Charleston Harbor, SC (Coast Guard), Davis-Monthan AFB, Tucson, AZ.

■ IA scans discovered correctable open ports and protocols, unneeded accounts and unnecessary services noted for correction in future releases.

IT 3.14

UNABRIDGED ASSESSMENT LINK

Coalition Secure Management and Operations System

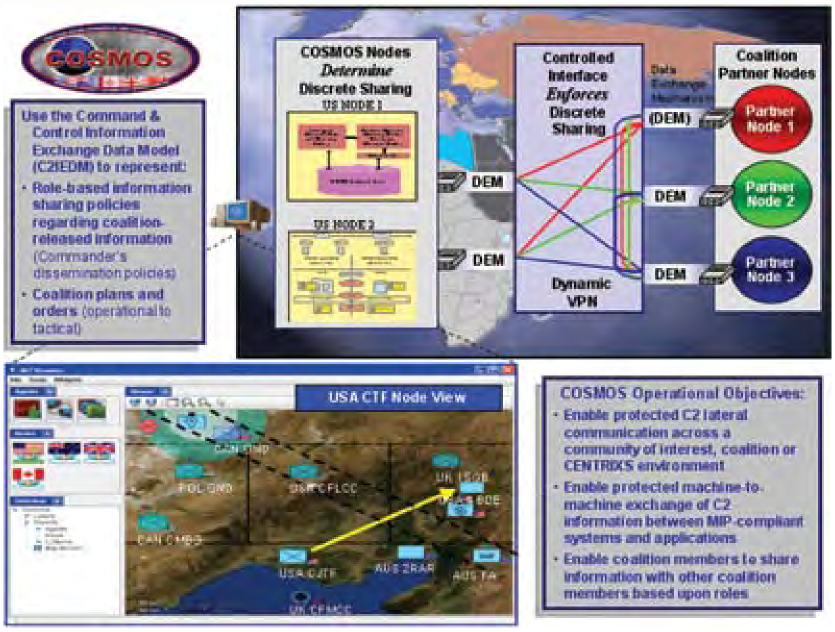
3. INTEGRATED OPERATIONS ● 6. INTEGRATED COMMUNICATIONS ●

TRIAL OVERVIEW: COSMOS enables protected and selected sharing of command and control (C2) information among coalition partners on a single coalition network leading to rapid and decisive operations. COSMOS provides automated information management, improves C2 operations support, enhances C2 information exchange security, and implements the Multilateral Interoperability Program (MIP) C2 Information Exchange Data Model (C2IEDM) and Data Exchange Mechanism (DEM). COSMOS exchanges locations, tracks, status, as well as distributes and displays orders and tasks. COSMOS reduces the risk for Multinational Information Sharing (MNIS) and service transition/integration capabilities.

SPONSOR:
OSD
USEUCOM
USPACOM
DISA

LOCATIONS:
USEUCOM
NSWC Dahlgren
Canada
New Zealand
United Kingdom

PARTNERS:
none



Use the Command & Control Information Exchange Data Model (C2IEDM) to represent:

- Role-based information sharing policies regarding coalition-released information (Commander's dissemination policies)
- Coalition plans and orders (operational to tactical)

COSMOS Operational Objectives:

- Enable protected C2 lateral communication across a community of interest, coalition or CENTRIXS environment
- Enable protected machine-to-machine exchange of C2 information between MIP-compliant systems and applications
- Enable coalition members to share information with other coalition members based upon roles

ASSESSMEMT RESULTS::
The COSMOS Trial operated on the CTF domains, receiving Warfighter, Technical Interoperability, and Basic Information Assurance (IA) assessments.

- COSMOS met CWID Objective 3 by passing C2 data in an international standard format (C2IEDM) between US, Canadian, and UK C2 systems.
- COSMOS demonstrated the ability to exchange and display track data received from both MIP-compliant (C2IEDM Format) and Non-MIP compliant C2 systems (OTH-Gold/ADAP P3 format). Although COSMOS was able to receive and display tracks received from MIP compliant systems, the trial was prevented from translating and forwarding C2IEDM formatted tracks to GCCS-J.
- COSMOS allowed MIP compliant systems to selectively share C2 data based on agreed upon sharing contracts and rule sets, allowing correct information to the correct coalition partner.
- No vulnerabilities found during a targeted IA assessment.

IT 3.22

UNABRIDGED ASSESSMENT LINK

Scalable Mesh Networks

3. INTEGRATED OPERATIONS ●

TRIAL OVERVIEW:OrderOne Networks (OON) provides a truly scalable Mobile Ad Hoc Network (MANET) protocol and a 3-D network visualization tool linked directly into the network. The MANET protocol supports 100,000's nodes and may be installed on virtually any device from sensors to handheld radios to vehicles and aircraft. The 3-D network visualization tool is for boots-on-the-ground personnel who need instant network situational awareness, including location of other nodes and their status, and who need the ability to communicate with the other nodes. OrderOne Networks also enables instant historical network activity review and node movements.

SPONSOR:
US Navy

LOCATIONS:
SPAWAR

PARTNERS:
none

ASSESSMENT RESULTS:
The OrderOne Networks Trial operated on HS/HD domain, receiving a Warfighter assessment and a SEIWG evaluation.

- OON provided excellent peer-to-peer connectivity, multi-casting, broadcast and distributed database functionality meeting CWID Objective 3 enhancing the commander's capability to command and control.
- OON successfully demonstrated a dynamic, self-healing, scalable mesh network of mobile packet-based devices utilizing minimal bandwidth and successfully connected to the HLS network from the MANET mesh network. OON allowed individual groups to network, communicate, and have their own Common Operating Picture showing all network members, maintaining full network functionality on a reduced scale.
- OON visualization tool provided additional benefit of a blue force tracking capability.

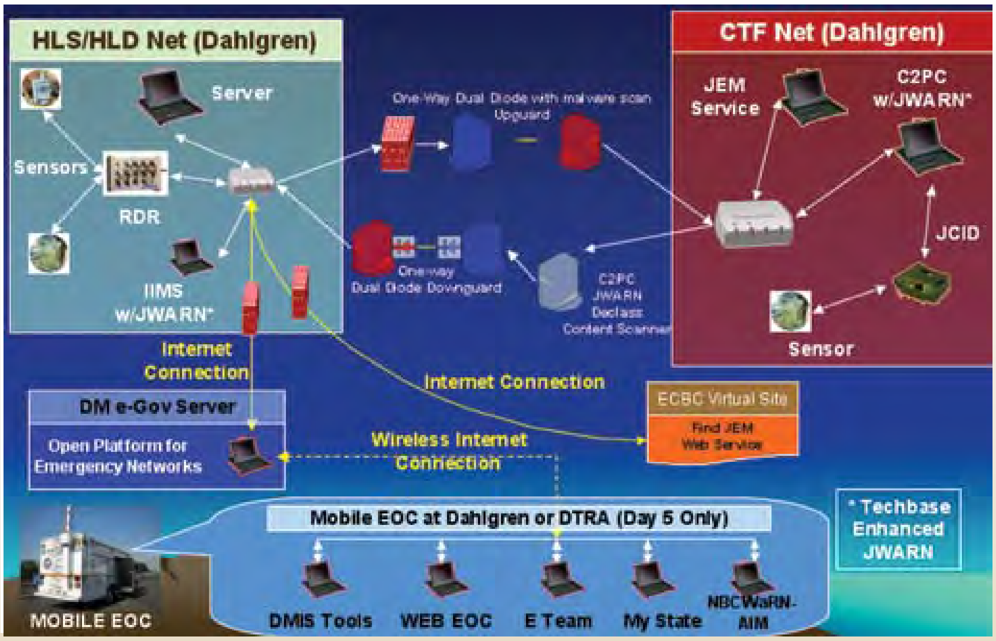
IT 3.27 UNABRIDGED ASSESSMENT LINK

Integrated Information Management System

1. CROSS DOMIAN DATA SHARING ● 3. INTEGRATED OPERATIONS ● 6. INTEGRATED PLANNING ●

TRIAL OVERVIEW: IIMS is an integrated hardware and software network which includes display of detector data, event management, hazard prediction, and CBRN hazard messaging. IIMS is interoperable with DoD C2 Systems and Emergency Management Alert Systems. IIMS uses a two-way guard for passing information both low to high and high to low and exchanges alerts with a civilian mobile Emergency Operation Center (EOC). The EOC shares alerts with Federal, State and local agencies through Open Platform Emergency Networks (OPEN). IIMS has evolved from the Restoration of Operations (RestOps) Advanced Concept Technology Demonstration (ACTD), Contamination Avoidance at Seaports of Debarkation (CASPOD) ACTD, and DTRA JSTO CBD Efforts.

SPONSOR:
US Air Force
LOCATIONS:
NSWC Dahlgren
PARTNERS:
IT 1.56



ASSESSMEMT RESULTS:
IIMS operated on the CTF and HS/HD domains, receiving Warfighter, Technical Interoperability, and Targeted Information Assurance (IA) assessments.

- IIMS successfully met CWID Objectives 1, 3, and 5, sharing CBRNE information with multiple civilian systems and the DoD GCCS/JWARN C2 system. IIMS used Dual Diode to pass USMTF and ADatP-3 v12 formatted messages to higher and lower security domains, converted, and forwarded civilian Common Alerting Protocol (CAP) Alert messages to DoD systems.
- Warfighters converted CAP messages into Emergency Action Reports and Situational Reports, sharing reports via e-mail to demonstrate interoperability and essential information sharing between disparate systems. This provided value in efficiently moving critical information.
- IA scans discovered correctable open ports and protocols, unneeded accounts and unnecessary services noted for correction in future releases.

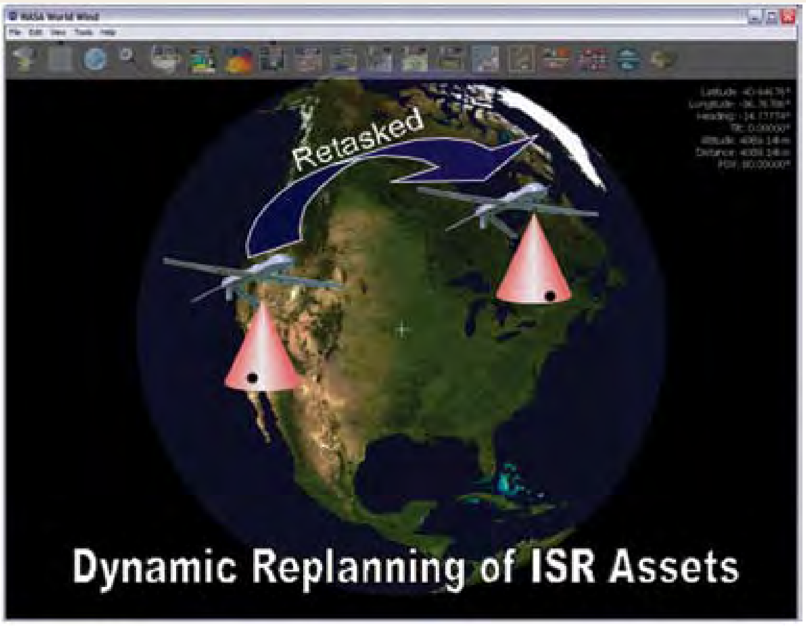
IT 3.30 UNABRIDGED ASSESSMENT LINK

Spatio-Temporal Analysis for Rapid Tasking

3. INTEGRATED OPERATIONS ●

TRIAL OVERVIEW: START enables warfighters to dynamically re-plan Intelligence, Surveillance and Reconnaissance (ISR) assets with improved situation awareness (SA), confidence, and target coverage. When an ISR asset is unexpectedly needed, e.g., for a Time-Sensitive Target (TST), START provides the decision-making environment to dynamically modify the current ISR schedule. By partnering human interaction with an asset-target pairing optimizer, users perform "what-if" analyses on asset re-tasking for dynamic and highly effective ISR operations.

SPONSOR:
US Air Force
LOCATIONS:
ESC Hanscom
PARTNERS:
none



ASSESSMENT RESULTS:
During CWID 2007, the START Trial operated on the CTF domain and received a Warfighter assessment and a SEIWG evaluation.

- START successfully met CWID Objective 3 by providing an ISR asset situational awareness tool with 3-dimensional graphics and drill-down displays that provided warfighters improved dynamic re-planning and re-tasking of ISR assets via insight into schedule optimization.
- START calculated and displayed ISR asset and mission planning options based on mission priorities, tasking, and schedules. The 3-dimensional graphic display provided ISR mission fly-through within the context of the global picture.
- Warfighters unfortunately did not have full confidence in START's ability to provide current, accurate and timely information because operators could not drill down on critical information nodes, such as, priorities, threats, and weather.

IT 3.31

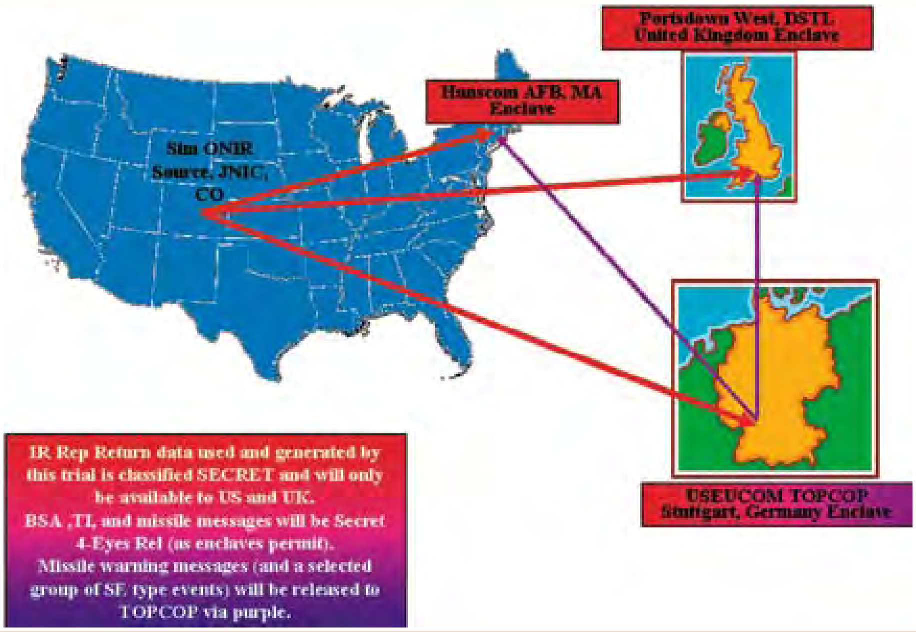
UNABRIDGED ASSESSMENT LINK

Coalition Infrared Data Processing

2. INTEGRATED INTELLIGENCE ● 3. INTEGRATED OPERATIONS ● 5. INTEGRATED PLANNING ●

TRIAL OVERVIEW: CIDP uses overhead non-imaging infrared sensors to expand the missile warning function that is historically provided by the Defense Satellite Program (DSP) System: battlespace awareness (battlefield activity and bomb damage assessment) and indications/warnings of changes in the battlefield (force redeployment and precursors to attack). CIDP provides joint exploitation (US & UK) of processed Space Based IR data for missile warning, battlespace awareness (BSA) and technical intelligence (TI) applications for use by the coalition warfighter for missile warning, missile defense, technical intelligence and battlespace awareness.

SPONSOR:
US Air Force
LOCATIONS:
USEUCOM
NSWC Dahlgren
United Kingdom
PARTNERS:
none



IR Rep Return data used and generated by this trial is classified SECRET and will only be available to US and UK.
BSA ,TI, and missile messages will be Secret 4-Eyes Rel (as enclaves permit).
Missile warning messages (and a selected group of SE type events) will be released to TOPCOP via purple.

ASSESSMEMT RESULTS:
The CIDP Trial operated on the CTF domain and received Warfighter, Technical Interoperability and Basic Information Assurance (IA) assessments.

- By providing improved data sharing with the US and UK C2 systems, CIDP met CWID Objectives 2, 3, and 5. CIDP provided data with minimal human intervention to both the GCCS-A, GCCS-J, and the ICS systems where data was correctly processed and displayed. The one drawback for CIDP was that the connection to GCCS-A and GCCS-J was performed with a serial connection and not sent via the typical network interface.
- CIDP demonstrated the ability to identify heat signatures and correlate them with imagery/known intelligence to improve the commanders' situational awareness in a variety of classified tactical situations.
- IA scans discovered correctable open ports and protocols, unneeded accounts and unnecessary services noted for correction in future releases.

IT 3.38

UNABRIDGED ASSESSMENT LINK

Collaborative Decision Aid

3. INTEGRATED OPERATIONS ● 5. INTEGRATED PLANNING ●

TRIAL OVERVIEW: CDA is an integrated suite of web-enabled software applications, presented in a web portal environment, and accessed via web browser. CDA supports synchronous conferencing and provides access to users at different access levels and disparate locations via the Internet, NIPRNET, or SIPRNET. CDA links decision makers in real-time to facilitate situational awareness "at a glance." Through a portal architecture, the CDA conferencing and decision support environment is accessed simultaneously at all levels: Federal, State or incident site. Decision makers, operational staffs and first responders can rapidly attain an identical level of situational awareness and understanding, quickly formulating decisions based on current emergency situations.

SPONSOR:
NGB
LOCATIONS:
USNORTHCOM
NSWC Dahlgren
PARTNERS:
none

ASSESSMENT RESULTS:
The CDA Trial operated on the HS/HD domain, receiving Warfighter, Technical Interoperability, and Basic Information Assurance (IA) assessments.

- CDA was moderately successfully meeting CWID Objectives 3 and 5. Through the CDA portal, users shared information on a common screen (including MPEG files) while directly linking multiple agencies to build real-time situational awareness.
- While users successfully accessed the CDA web-based portal to collaborate using chat, white boarding, and file sharing, the CDA trial could not demonstrate the VoIP capability between USNORTHCOM and Dahlgren. The VoIP issue was likely due to an unresolved network issue and workstations not having the correct Java settings. Coupled with GUI issues, the warfighter's ability to utilize the tool's full potential was hampered.
- IA scans discovered open ports and protocols, unneeded accounts and unnecessary services that required closure.

IT 3.39

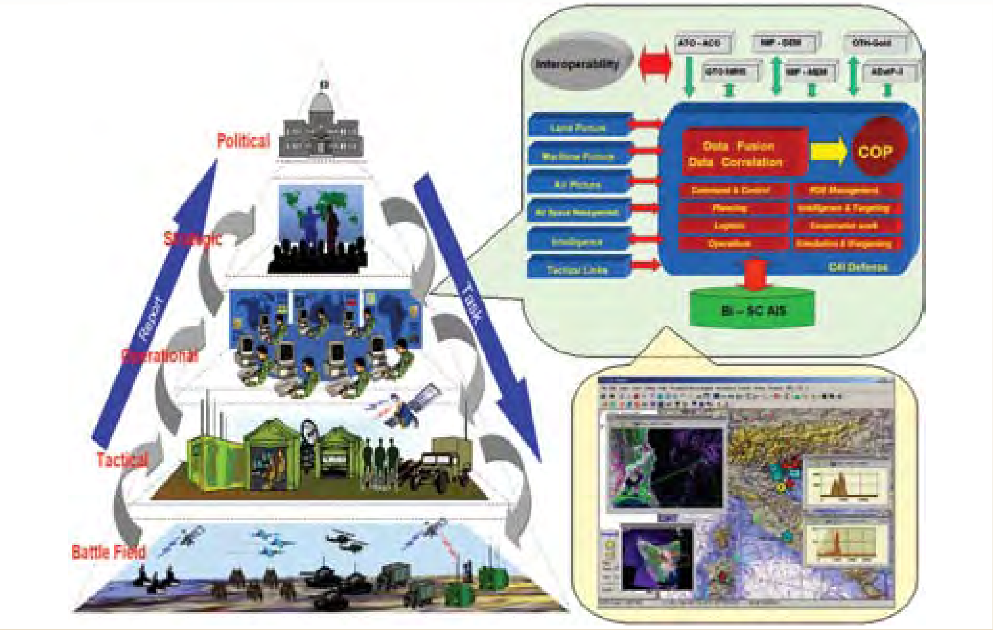
UNABRIDGED ASSESSMENT LINK

Command, Control, Communication, Computers and Intelligence Defence

3. INTEGRATED OPERATIONS ●

TRIAL OVERVIEW: Italian C4I Defence joint system provides top-level strategic capabilities, laying above the tactical functionalities offered by the C2 systems of each Service as well as data and information exchanging capabilities with other NATO/PfP/US, joint and single service C2 systems. The system supports high level C2 capability and COP exchanging in a multilateral environment, through formatted messages in OTH-Gold, ADatP-3 and USMTF 2000 standards, improving situational awareness in a multinational environment.

SPONSOR:
Italy
LOCATIONS:
USEUCOM
NSWC Dahlgren
ESC Hanscom
Canada
PARTNERS:
none



ASSESSMENT RESULTS:
The C4I Defence Trial operated on the CTF domain, receiving a Technical Interoperability assessment.

■ C4I Defence successfully met CWID Objective 3 by exchanging track data with US C2 systems GCCS-J and TBMCS, demonstrating an enhancement to existing technology that streamlines the operational decision-making process.

■ C4I Defence sent JUNIT messages to GCCS-J that were processed and displayed within the US TOP COP and received and processed USMTF formatted ATO and ACO messages from TBMCS and CTC OTH-Gold formatted messages from GCCS-J.

■ Unsuccessful exchanges with Canadian TBMCS were linked to a planning issue, not a C4I Defence Trial problem. Other minor issues with simulated messages showed unrecognized code in the sensor field (not a C4I Defence trial issue) that was quickly resolved by changing the contents of the field from OTHR to OTH.

IT 3.48

UNABRIDGED ASSESSMENT LINK

Air Support Operations Center with Close Air Support System

3. INTEGRATED OPERATIONS ●

TRIAL OVERVIEW: The ASOC Gateway provides the capability to tie all Joint Tactical Air Controllers (JTACs) on the battlefield with digital network aircraft (Link 16/SADL). The CASS software itself, without the use of the gateway, has direct line-of-site digital communications with FA-18s, AV-8Bs, and F-16s. This capability is being expanded to aircraft such as the A-10, B-52, and Network Enabled Weapons such as Small Diameter Bomb.

SPONSOR:
US Air Force
LOCATIONS:
NSWC Dahlgren
PARTNERS:
none

ASSESSMENT RESULTS:
The CASS Trial operated on the CTF domain, receiving Warfighter and Technical Interoperability assessments.

■ ASOC Gateway successfully met CWID Objective 3 by providing tools to assess tactical air operations, assign aircraft, and approve Air Support Requests.

■ Warfighters received a Link-16 picture through UAV video feed using a Remotely Operated Video Enhanced Receiver (ROVER) via a JREAP-C connection between Hanscom and Dahlgren.

■ ASOC Gateway, running on the Moving Map Tactical Information Display System, successfully streamlined decision making by providing a graphical picture of the situation, and improved blue force tracking.

■ ASOC Gateway demonstrated dismounted role players using the Laser Range Finder (LRF) capability to capture and transmit target locations (lat/long), automatically sent via UHF as textual data to CASS software for display.

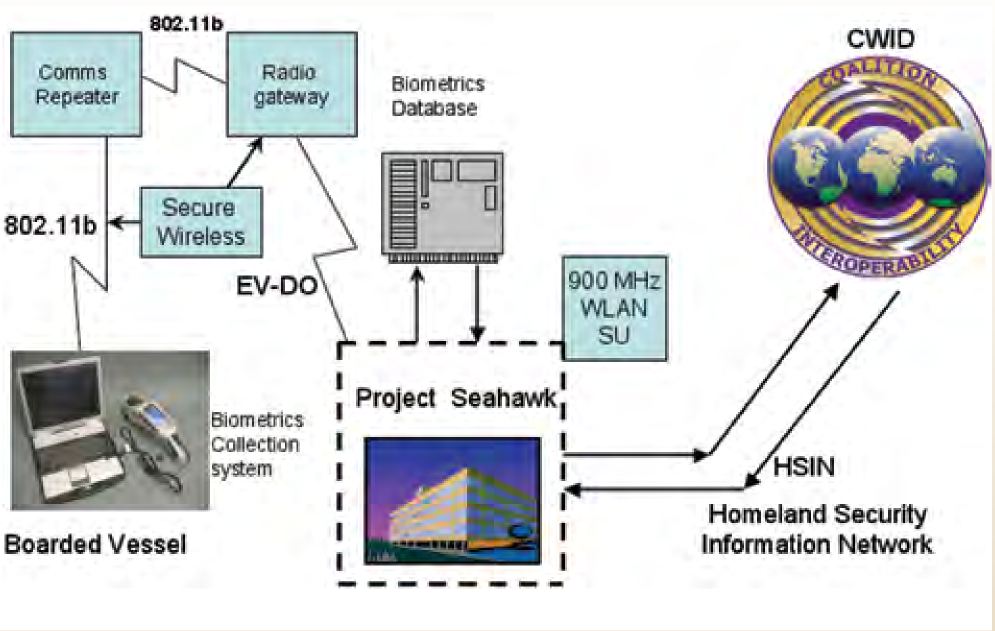
IT 3.58 UNABRIDGED ASSESSMENT LINK

U.S. Coast Guard Information Sharing & Communications

3. INTEGRATED OPERATIONS ●

TRIAL OVERVIEW: USCG IS&C provides a rapid and secure means of communicating from vessels off shore to the local command centers. It solves a long-standing problem maintaining communications with boarding teams and works even when the boarding team is deep within a large ship. It also provides rapid and secure transmission of biometric (fingerprint) data results and database comparisons to command centers, high-level operational commanders, federal government agencies, state and local agencies. USCG IS&C provides a substantial improvement in situational awareness to appropriate command and control entities through a netcentric community of interest (COI).

SPONSOR:
US Coast Guard
LOCATIONS:
USNORTHCOM
NSWC Dahlgren
South Carolina
PARTNERS:
none



ASSESSMENT RESULTS:
USCG IS&C operated on the HS/HD domain, receiving a Warfighter assessment, a Basic Information Assurance (IA) assessment and a SEIWG evaluation.

- USCG IS&C successfully met CWID Objective 3 by establishing an encrypted mesh wireless network from ship to shore communications for securing biometric data exchange.
- USCG IS&C rapidly and securely exchanged information (VoIP, Video, Audio) between USCG assets and external commands while establishing a secure command structure for USCG boarding parties.
- While the USCG IS&C permits boarding team communications throughout the ship, the current design is somewhat cumbersome for a boarding team's quick agile movements.
- IA scans discovered correctable open ports and protocols, unneeded accounts and unnecessary services noted for correction in future releases.

IT 3.70 UNABRIDGED ASSESSMENT LINK

Coalition open Joint Operations Picture

3. INTEGRATED OPERATIONS ● 5. INTEGRATED PLANNING ●

TRIAL OVERVIEW: CoJOP is the coalition deployment of openJOP that delivers the Joint Operations Picture (JOP) on the (UK) Defence Information Infrastructure (DII). The trial's ability to generate, access and protect information, and its ability to share it throughout the network, allows force elements to operate from common data sets (or 'pictures') of operational information. Consistent throughout the operating space, operational information data sets draw on the same underlying environmental and reference information. The JOP consists of the Common Operations Picture (COP) and JOP-Web, a tool that, amongst other things, collates operational reports that reflect the most current information.

SPONSOR:
United Kingdom
LOCATIONS:
USEUCOM
NSWC Dahlgren
SPAWAR
ESC Hanscom
New Zealand
United Kingdom
PARTNERS:
IT 2.88

ASSESSMENT RESULTS:
During CWID 2007, the CoJOP Trial operated on the CTF domain and received a Warfighter and a Technical Interoperability assessment.

- CoJOP was moderately successfull meeting CWID Objectives 3 and 5. Insufficient training, inadequate technical support, configuration/set-up issues, access issues, and uncompleted MSELs were factors in the trials overall effectiveness/success.
- Role players were successful accessing the air and maritime picture using the WebS2AT and the Land Picture through the CoJOP SITAWARE. Additionally, CoJOP used resources from Jane's Information Group, Ltd., UK, as a data source.

IT 3.71 UNABRIDGED ASSESSMENT LINK

MobiKEY Identity Based Access Drive & Defense Identity Management Network

3. INTEGRATED OPERATIONS ● 5. INTEGRATED PLANNING ●

TRIAL OVERVIEW: MobiKEY IBAD and DEFIMNET infrastructure provide military users with the combination of ease-of-use and strong cryptography required for in-theater operations. MobiKEY IBAD's thumb-sized form factor, coupled with strong multi-factor identification and sophisticated entitlement controls, ensures warfighters secure access to the systems and information they need, when and where they need it. The data is never exposed outside of the headquarters' secured network. When using existing battlefield or naval networks for connectivity, warfighters simply plug their MobiKEY IBAD into a PC for instant access to systems at HQ or at their home command. MobiKEY IBAD can be deployed in both the unclassified and classified domains.

SPONSOR:
Canada
LOCATIONS:
USEUCOM US-NORTHCOM
NSWC Dahlgren
SPAWAR
ESC Hanscom
Canada
New Zealand
PARTNERS:
none

ASSESSMEMT RESULTS:
MobiKEY operated on the CTF and HS/HD domains, receiving Warfighter, Technical Interoperability, and Targeted Information Assurance (IA) assessments.

■ MobiKEY IBAD successfully met CWID Objectives 3 and 5 by providing secure remote access to systems and information in an easier and more flexible manner, enhancing coalition information sharing among allies and coalition partners.

■ Role players accessed their personal host using the MobiKEY encrypted device, demonstrating quick cryptographic device disbanding (5 seconds). Applications accessed were Outlook send/receive with attachments, Excel, Word, PowerPoint, and Click-to-Meet.

■ Role players demonstrated MobiKEY SIM card destruction after 4 unsuccessful incorrect password access attempts.

■ IA scans discovered correctable open ports and protocols, unneeded accounts and unnecessary services noted for correction in future releases.

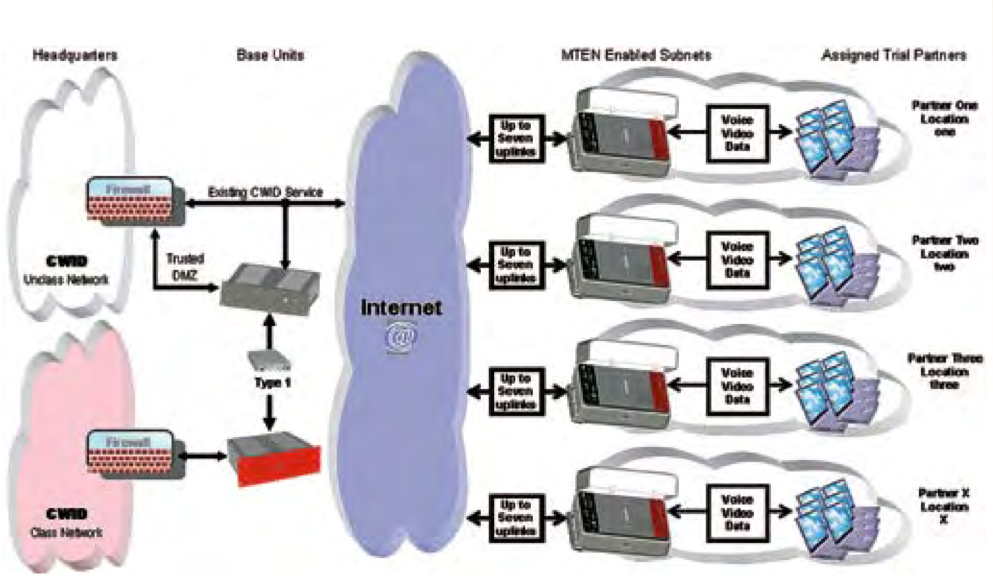
IT 3.75 UNABRIDGED ASSESSMENT LINK

Mobile Tactical Edge Network

3. INTEGRATED OPERATIONS ●

TRIAL OVERVIEW: The pTerex MTEN solution enables information sharing at all levels of coalition command. The products are secure, scaleable, and functional at all levels of warfare. MTEN is nonproprietary and was successfully tested for integration and interoperability by US Joint Forces Command (USJFCOM), Naval Special Warfare Command (NAVSPECWARCOM), and Joint Systems Integration Command (JSIC). MTEN products are middleware equipment enabling connection to home networks regardless of location. A lightweight, rugged equipment solution, MTEN provides means to collaborate with existing software and bandwidth capabilities. MTEN manages global roaming of mobile networks among and between virtually any current or future network: wired, cellular, 802.11b/g wireless, radio and satellite.

SPONSOR:
USNORTHCOM
LOCATIONS:
USEUCOM
USNORTHCOM
NSWC Dahlgren
South Carolina
West Virginia
PARTNERS:
none



ASSESSMENT RESULTS:
The pTerex MTEN Trial operated on the HS/HD domain, receiving Warfighter, Technical Interoperability, and Targeted Information Assurance (IA) assessments.

■ PTerex successfully met CWID Objective 3 by providing a wired/wireless infrastructure for users at USEUCOM, USNORTHCOM and Dahlgren to hold Click- to-Meet collaboration VTCs. VTC audio was very good and video was fair with intermittent latency.

■ Following a main power interruption, role players continued to search and download data via the internet with no visible service degradation due to pTerex's 4 hour battery backup capability.

■ An incredible asset to the warfighter (vehicle) and commander (case unit), pTerex greatly enhanced mission operations through its mobility and ability to keep clients connected.

■ IA scans discovered open ports and protocols that require closure for future demonstration.

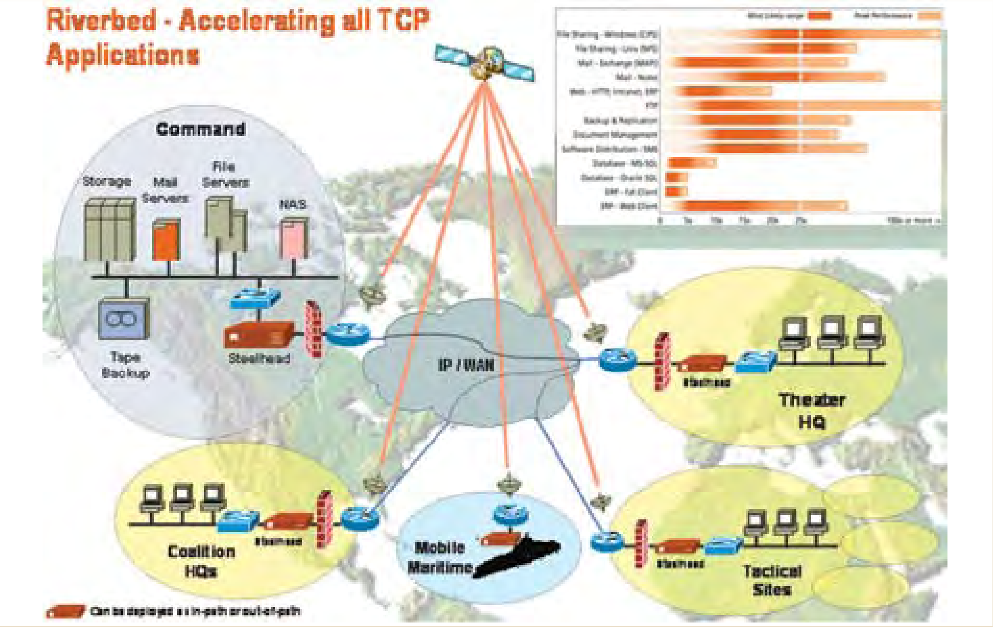
IT 3.80 UNABRIDGED ASSESSMENT LINK

Riverbed Information Optimization System

3. INTEGRATED OPERATIONS ● 4. INTEGRATED LOGISTICS ●

TRIAL OVERVIEW: RIOS is high performance and scalable, optimizing all Transmission Control Protocol (TCP) traffic for maximum bandwidth. Additional application-specific optimizations further enhance response times. RIOS uses a new combination of patented and patent-pending mechanisms to achieve application acceleration. These mechanisms include transaction prediction, TCP proxying and optimization, and hierarchical compression to deliver orders of magnitude increases in application response time and throughput.

SPONSOR:
US Air Force
DISA
LOCATIONS:
USEUCOM
NSWC Dahlgren
ESC Hanscom
PARTNERS:
none



ASSESSMEMT RESULTS:
The RIOS Trial operated on the CTF domain, receiving Warfighter, Technical Interoperability, and Basic Information Assurance (IA) assessments.

- RIOS successfully met CWID Objective 3 by demonstrating a more rapid file transfer capability in a busy network environment with the RIOS Accelerator Optimizer. File types optimized were MS Word and email with large imagery attachments.
- Originally scheduled to operate on both the HS/HD and Coalition networks, RIOS withdrew from the HS/HD domain. MSEL inefficiencies also precluded RIOS from demonstrating CWID Objective 4.
- Lack of technical support at sites hindered the RIOS demonstration. Warfighters said the technology was too technical and not intuitive enough to operate without more guidance.
- IA scans discovered correctable open ports and protocols, unneeded accounts and unnecessary services noted for correction in future releases.

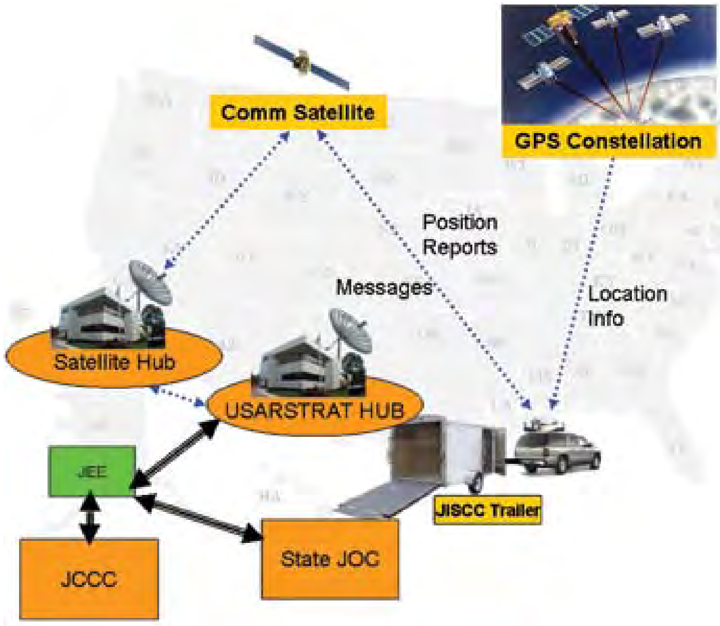
IT 4.79 UNABRIDGED ASSESSMENT LINK

Event-based Common Operational Picture

3. INTEGRATED OPERATIONS ● 4. INTEGRATED LOGISTICS ● 5. INTEGRATED PLANNING ●

TRIAL OVERVIEW: National Guard Bureau's (NGB) Joint CONUS Communications Support Environment (JCCSE) is an umbrella concept including communications and information systems that provide connectivity, collaboration, situational awareness, and C4 coordination between Homeland Defense (HD) and Defense Support to Civil Authorities (DSCA) mission partners. Event-based Common Operational Picture (E-COP) provides Geospatial Information Systems (GIS) visualization of common operational event and asset data, using standards-based tools and symbology. It shares geo-referenced event and asset data with all mission partners, supports improved coordination of distributed operations, and enables the NGB Joint C4 Coordination Center (JCCC) to improve coordination and employment of C4 Assets in response to multiple events.

SPONSOR:
National Guard Bureau (NGB)
LOCATIONS:
USNORTHCOM
NSWC Dahlgren
SPAWAR
ESC Hanscom
South Carolina
West Virginia
PARTNERS:
none



ASSESSMENT RESULTS:
During CWID 2007, the NG-ECOP Trial operated on the HS/HD domain and received a Warfighter and, Technical Interoperability assessment.

- NG-ECOP successfully demonstrated CWID Objectives 3, 4, and 5 when role players used the Triton web-based portal situational awareness display to identify locations and check the C4 asset status near the affected region. Displayed asset icons were accompanied by easy access to detailed information for the particular asset. This essential information improved planning capabilities supporting HS/HD scenarios and operations.
- Inadequate training at SPAWAR San Diego prevented a full demonstration of NG E-COP capabilities at that location and precluded an accurate evaluation from the SPAWAR warfighter. Training was not an issue from warfighters at other sites.

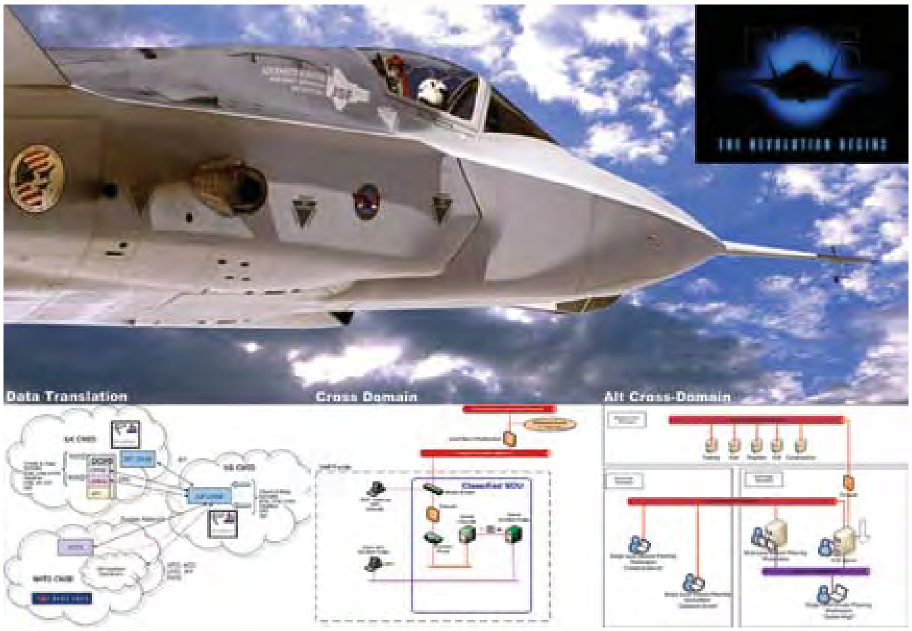
IT 5.08 UNABRIDGED ASSESSMENT LINK

Joint Strike Fighter Offboard Mission Support Environment

1, CROSS-DOMAIN DATA SHARING ● 5. INTEGRATED PLANNING ●

TRIAL OVERVIEW: The Joint Strike Force (JSF) is a multinational endeavor to develop a common fighter aircraft. OMSE is the JSF's ground-based mission planning system. The OMSE is designed to support all aspects of coalition mission preparation and post mission analysis. JSF provides the ability to translate JSF partner country mission planning non-US data into the JSF OMSE and to translate JSF mission planning data to JSF country specified non-US data. The benefit is the one mission planning system that will fulfill U.S. and JSF partner mission planning utilizing country specific data, providing cost benefits and data transparency between countries. JSF gives a new user GUI to mission planning that allows users a more understandable interface as well as less button click formats.

SPONSOR:
Joint Strike Fighter (JFS) Program Office
LOCATIONS:
NSWC Dahlgren
ESC Hanscom
United Kingdom
PARTNERS:
none



ASSESSMEMT RESULTS:
The JSF OMSE Trial operated on the CTF and CTF High domains, receiving Warfighter, Technical Interoperability, and Basic Information Assurance (IA) assessments.

- JSF OMSE successfully met CWID Objective 1, simplifying mission data transfer from low to high using a small footprint. The system performed well, is combat ready, and is an improvement over previous systems.
- JSF OMSE met CWID Objective 5, receiving and translating UK ADatP-3 formatted ACO/ ATOs into USMTF2000 for users to identify task and unit information, receive and process Friendly Order of Battle (FrOB) information from JOP (a UK database) and convert elements of the FrOB database into US format through a "data map." JSF OMSE displayed them as images showing enemy targets.
- IA scans discovered correctable open ports and protocols, unneeded accounts and unnecessary services noted for correction in future releases.

IT 5.12 UNABRIDGED ASSESSMENT LINK

ID-MAP: Situational Awareness, Visualization and Collaboration

2. INTEGRATED INTELLIGENCE ● 3. INTEGRATED OPERATIONS ● 5. INTEGRATED PLANNING ●

TRIAL OVERVIEW: ID-Map (IC-1) allows multiple users in different locations to collaborate by seeing what others see, automatically sharing each others' information, maps, reports, data, writings, notations, and geospatial images, from most any source — to virtually see what others are thinking. ID-Map (IC-1) provides a collaborative environment for Domain Awareness, allowing disparate users to share and analyze information in real-time. ID-MAP is built on CoMotion®, a real-time, decision-making "always on" dynamic, collaborative environment platform. ID-MAP enables decision makers with actionable intelligence to cross multiple boundaries in real time using collaboration, visualization and analysis.

SPONSOR:
USNORTHCOM
US Coast Guard
LOCATIONS:
USNORTHCOM
NSWC Dahlgren
SPAWAR
PARTNERS:
none

REAL-TIME COLLABORATION
COMMUNICATIONS
RESOURCE ALLOCATION
THREAT INTELLIGENCE
SURVEILLANCE
PLANNING & MISSION REFINEMENT
INTERDICTION

ASSESSMENT RESULTS:
The ID-MAP Trial operated on the HS/HD domain, receiving Warfighter, Technical Interoperability, and Targeted Information Assurance (IA) assessments.

- ID-Map IC-1 successfully met CWID Objectives 2, 3, and 5 by providing a collaborative environment allowing disparate users to plan, share, analyze and communicate real-time using chart visualization, maps, reports, intelligence, and other data, coordinating command and control collaboration efforts. Users employed the VoIP feature (CrossComm) for collaboration. They shared intelligence within moments of a situation.
- ID-MAP received and incorporated various track inputs to the HS/HD COP, providing geospatial position data on ground assets augmented with AIS vessel data attributes for vessels outfitted with an AIS transponder.
- IA scans discovered open ports and protocols, unneeded accounts and unnecessary services that required closure.

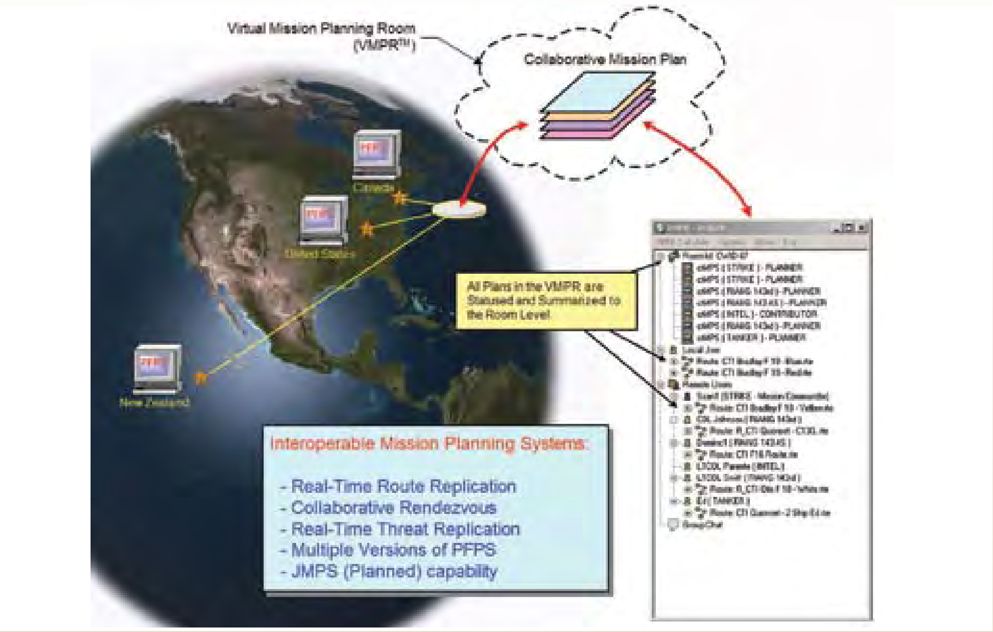
IT 5.59 UNABRIDGED ASSESSMENT LINK

Mission Planning System

3. INTEGRATED OPERATIONS ● 5. INTEGRATED PLANNING ●

TRIAL OVERVIEW: MPS is a collaboration-enabled Portable Flight Planning System (PFPS) which allows users to enter a Virtual Mission Planning Room (VMPR). It is simple to use, requiring little additional training beyond operational familiarity with PFPS. MPS provides new capabilities to the mission planner, allowing geographically separated warfighters to collaborate in real time. MPS also provides intelligence to create, input and share threat data symbology, greatly enhancing situational awareness. Once in a VMPR, each user works on routes and observes routes created and updated by other users in the virtual room. The slightest change to a route immediately reflects in the VMPR. The MPS Collaborated Rendezvous capability automates steps for creating refueling and mission support rendezvous.

SPONSOR:
US Air Force
LOCATIONS:
ESC Hanscom
NATO
Canada
New Zealand
PARTNERS:
none


Virtual Mission Planning Room (VMPR™)
Collaborative Mission Plan
Canada
United States
New Zealand
All Plans in the VMPR are Statused and Summarized to the Room Level
Interoperable Mission Planning Systems:
- Real-Time Route Replication
- Collaborative Rendezvous
- Real-Time Threat Replication
- Multiple Versions of PFPS
- JMPS (Planned) capability
cMPS (STRIKE) - PLANNER
cMPS (STRIKE) - PLANNER
cMPS (INTEL) - CONTRIBUTOR
cMPS (TANKER) - PLANNER
Local User
Remote Users
GroupChat

ASSESSMENT RESULTS:
The MPS Trial operated on the CTF domain, receiving Warfighter and Technical Interoperability assessments.

■ MPS met CWID Objectives 3 and 5, allowing concurrent air mission planning in virtual rooms by nation, service or coalition. Using the Package Commander application, MPS dramatically decreased mission planning process time and facilitated an easy route assessment/de-confliction process.

■ MPS established collaborative information and task sharing environments to adjudicate pre-flight mission planning, immediate air route de-confliction analysis, and post flight assessments. Enabling multiple units to coordinate routes, times, refueling, and threats in real time environment, it streamlined operational decision making.

■ MPS also integrated disparate system software applications and air data sources together for coalition and federated interoperability.

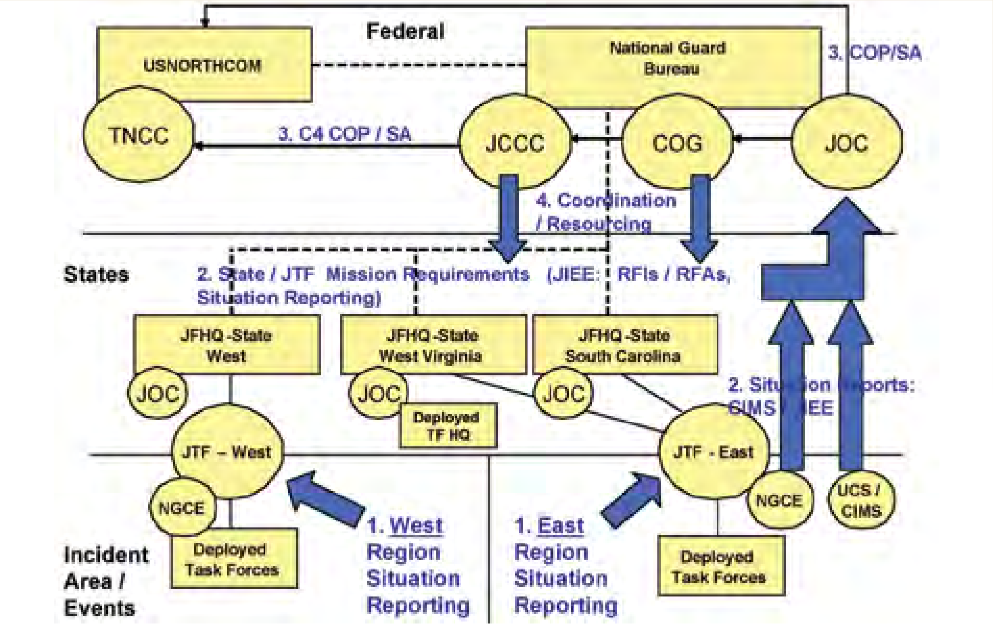
IT 5.78 UNABRIDGED ASSESSMENT LINK

Next Generation-Joint Information Exchange Environment

5. INTEGRATED PLANNING ●

TRIAL OVERVIEW: NGB's JCCSE is an umbrella concept enabling the reliable and timely flow of key information to support state and Federal military activities for Homeland Defense (HD) and Defense Support to Civil Authorities (DSCA). It includes communications systems and programs that provide connectivity, collaboration, situational awareness, and C4 coordination. JIEE is the JCCSE component supporting information sharing and critical processes, such as tracking and situation reporting. NG-JIEE improves situation-reporting capabilities that support Essential Elements of Information (EEIs) for support to HD/DSCA missions. NG-JIEE supports technology evaluations and processes supporting collection and information dissemination across the National Guard and with mission partners focusing on net-centric solutions.

SPONSOR:
National Guard Bureau (NGB)
LOCATIONS:
USNORTHCOM
NSWC Dahlgren
SPAWAR
ESC Hanscom
South Carolina
West Virginia
PARTNERS:
none



ASSESSMENT RESULTS:
The NG-JIEE Trial operated on the HS/HD domain, receiving Warfighter, Technical Interoperability and Basic Information Assurance (IA) assessments.

■ NG-JIEE successfully demonstrated CWID Objective 5 by permitting users to track and share event data. Role players entered event information in the JIEE logs, automatically sending emails to other battle staffs.

■ While role players could attach messages into JIEE, they could not manipulate the attachment once uploaded to JIEE without saving the document as a word file then uploading it as an active event for informational purposes.

■ JIEE is a solid program but, requires some improvements with group/subgroup sharing, GUI improvements, manual search of events regardless of domains, linking of RFI's and RFA's to events and an interactive map.

■ Basic IA scan showed all required patches not installed.

IT 6.04

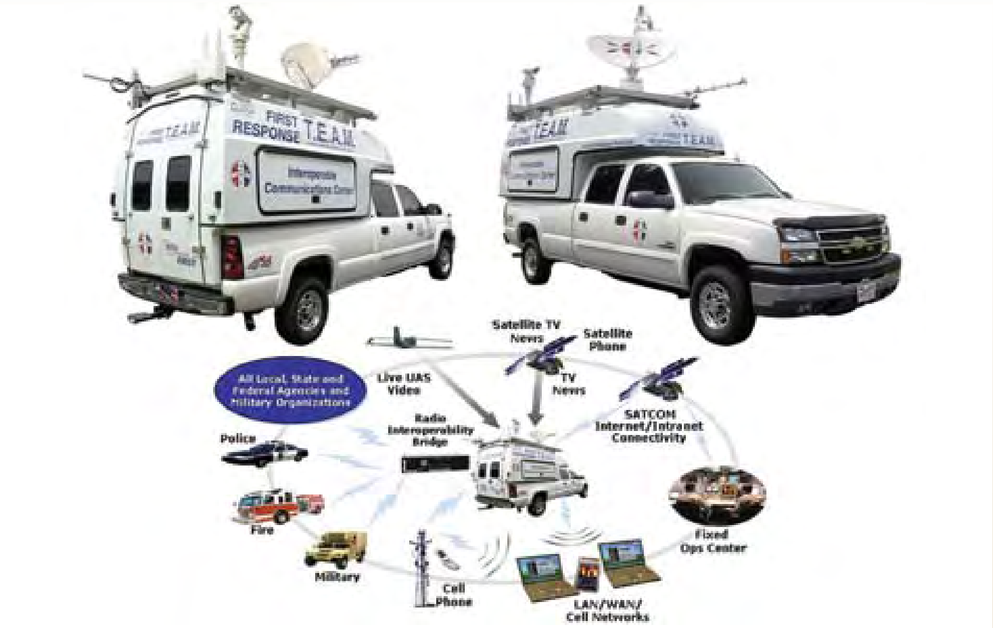
UNABRIDGED ASSESSMENT LINK

Tactical Emergency Asset Management System

6. INTEGRATED COMMUNICATIONS ●

TRIAL OVERVIEW: The T.E.A.M. system is a small-footprint, self-deployable system providing net-centric communications for incident commanders and for communications between operational and tactical levels of activity. It provides the means to synchronize and connect federal, state, local and non-governmental agencies and organizations with each other and with military organizations to provide an integrated and fused common operational picture to interagency partners. The system bridges civilian first responder radios and land-line, cellular and satellite telephone communications, providing integration between civil first response and military radios, satellite broadband internet data connectivity, VoIP and video streaming, wireless access, satellite television, public address systems, and on-board power generation.

SPONSOR:
USNORTHCOM
LOCATIONS:
USNORTHCOM
SPAWAR
South Carolina
West Virginia
PARTNERS:
none


FIRST RESPONSE T.E.A.M.
Interoperable Communications Center
T.E.A.M.
Satellite TV News
Satellite Phone
All Local, State and Federal Agencies and Military Organizations
Live UAS Video
TV News
Radio Interoperability Bridge
SATCOM Internet/Intranet Connectivity
Police
Fire
Military
Cell Phone
LAN/WAN/ Cell Networks
Fixed Ops Center

ASSESSMEMT RESULTS:
The T.E.A.M. Trial operated on the HS/HD domain, receiveing Warfighter and Technical Interoperability assessments.

■ T.E.A.M. successfully met CWID Objective 6 by quickly setting up a communications center and bridging radios using the Raytheon ACU-1000. T.E.A.M. also provided continuous video feed to users on the CWID HS/HD network via a web-based video server.

■ T.E.A.M. planned to demonstrate CWID Objective 5 with all applicable users on the HS/HD network using SKYPE. However, connectivity permissions into the SPAWAR site, only allowed T.E.A.M. to use SKYPE to collaborate, which included video, audio, whiteboard and text chat, between users within the T.E.A.M. vehicles.

■ The T.E.A.M. system supported county Emergency Operations Centers (EOCs) in West Virginia and South Carolina, quickly filling voids in connectivity and providing situational awareness at all levels.

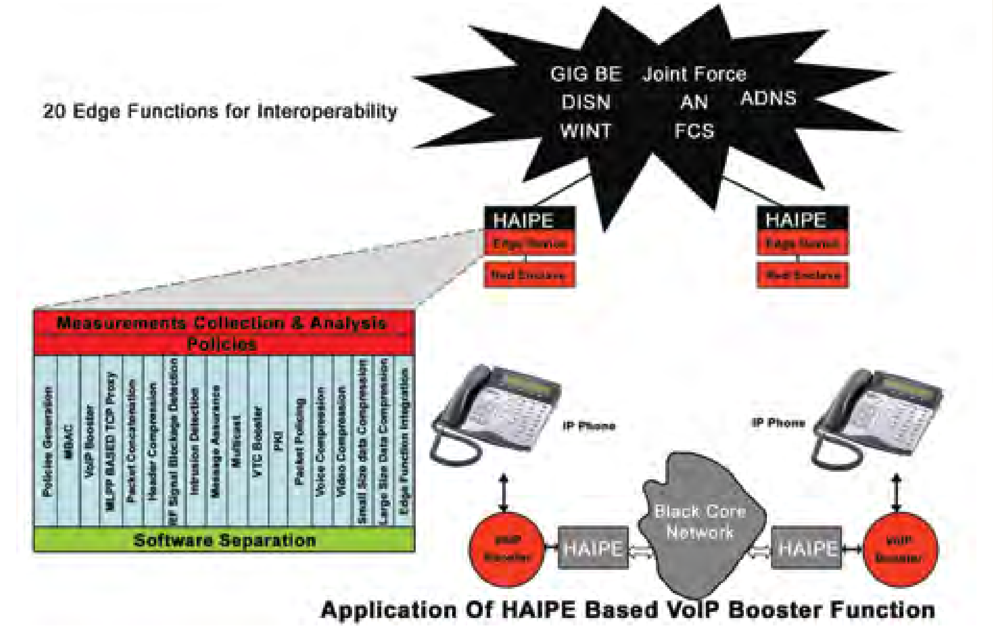
IT 6.13

Global Information Grid Quality of Service Edge Solution for Interoperability

6. INTEGRATED COMMUNICATIONS ●

TRIAL OVERVIEW: GIG QoS ESI is an edge solution, integrated into an application or as a stand-alone product that provides Interoperability of applications across multiple networks. Using QoS, signaling between edge devices provides consistency cross the GIG. QoS is a TACLANE-based solution that meets all NSA standards of encryption. The edge solutions mitigate much of the network degradation that warfighters experience while communicating during travel through dense foliage or an urban area. The VoIP booster allows a warfighter to communicate voice in a reliable way even when the packet loss ratio is very high (close to 50%).

SPONSOR:
US Army
LOCATIONS:
NSWC Dahlgren
SPAWAR
New Zealand
PARTNERS:
none



ASSESSMENT RESULTS:
Due to technical issues during set-up week, the GIG QoS ESI Trial withdrew from the demonstration during execution.

■ GIG QoS ESI failed to achieve its stated objective of Integrated Communications. Unable to connect to the CTF network or properly configure the SATSIM to operate effectively, GIG QoS ESI withdrew from CWID as an Interoperability Trial during week one of CWID execution.

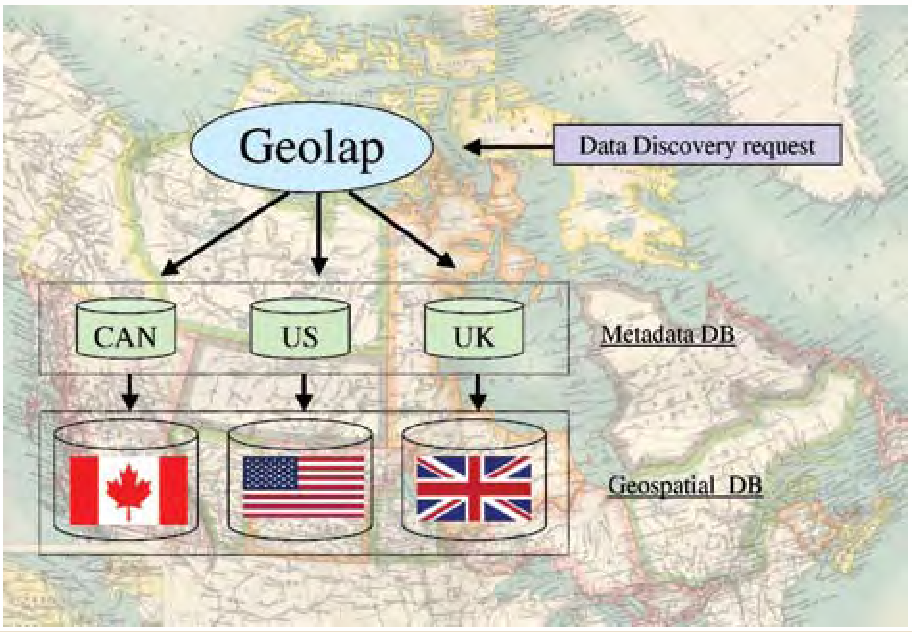
IT 6.15 UNABRIDGED ASSESSMENT LINK

Geolap

6. INTEGRATED COMMUNICATIONS ●

TRIAL OVERVIEW: GEOLAP is a Defense Research and Development Canada (DRDC) Valcartier application developed to track production statistics and provide drill down query capability on the production management information for the NTDB (National Topographic Database). Geolap implements Online Analytical Processing (OLAP) technology which provides improvements in overall performance. Functionalities include geospatial data search tools and discovery and dissemination capabilities based on ISO 19115 metadata standards.

SPONSOR:
Canada
LOCATIONS:
USNORTHCOM
Canada
United Kingdom
PARTNERS:
none



ASSESSMEMT RESULTS:
During CWID 2007, the GeoLap Trial operated on the CTF domain and received a Warfighter assessment.

- Geolap successfully met CWID Objective 6 of enhancing coalition information and knowledge sharing capabilities among allies and coalition partners by providing a web-based tool with the ability to search and view geospatial data products through a metadata database.

- Generally, warfighters found the tool easy to use but not very intuitive. They also found the tool was slow to respond when navigating the site. Even though Geolap successfully demonstrated its capabilities, warfighters felt that its functionalities were very basic and needed to be improved before it was ready for deployment.

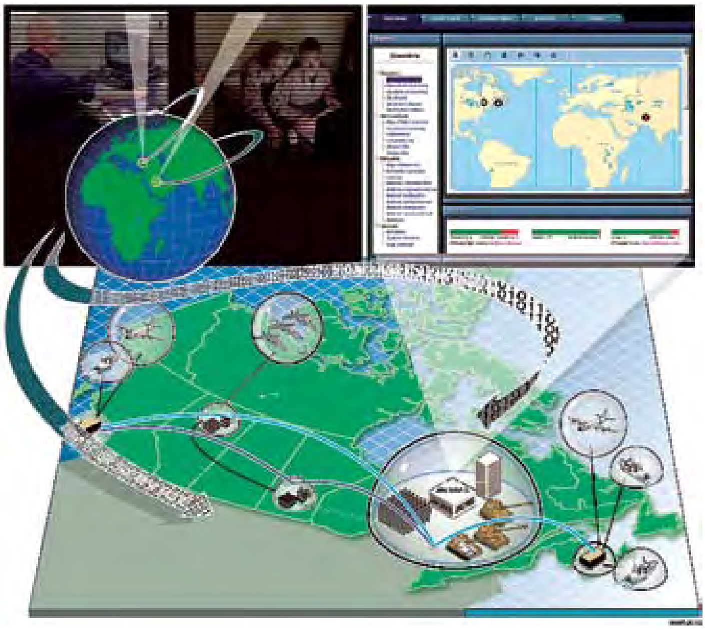
IT 6.36 UNABRIDGED ASSESSMENT LINK

Joint Network Defense and Management System

6. INTEGRATED COMMUNICATIONS ●

TRIAL OVERVIEW: JNDMS is an integration, analysis and monitoring system that provides situational awareness for computer network defense (CND). The JNDMS focuses on providing decision makers the right network information at the right time. JNDMS is operation-centric and collects, fuses, and displays data from multiple domains. Data sources include network management sensors, network security sensors, and various databases. The displayed information allows users to understand the state of the networks. JNDMS assesses the severity and impact on military operations of network incidents and includes a geospatial view of networks.

SPONSOR:
Canada
LOCATIONS:
Canada
PARTNERS:
none



ASSESSMENT RESULTS:
During CWID 2007, the JNDMS Trial operated on the CTF domain received a Warfighter assessment.

- JNDMS successfully met CWID Objective 6 of enhancing coalition information and knowledge sharing capabilities through an integration analysis and monitoring system that provided network situational awareness and allowed commanders and network analysts to assess the impact of network events on military operations.

- Overall, warfighters found that JNDMS worked well and that after some hands-on interaction, JNDMS was easy to use. The system was stable and reliable during CWID execution, but its performance ability was slow. JNDMS is a promising tool that, with further development, could provide value for both network analysts and other watch officers.

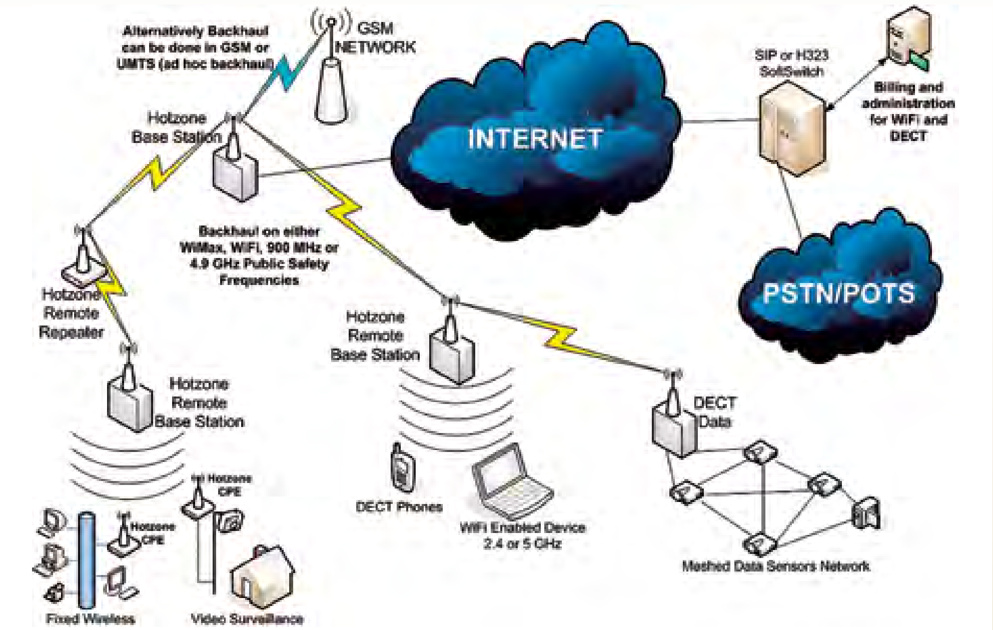
IT 6.42 UNABRIDGED ASSESSMENT LINK

HotZone 4010/4020

3. INTEGRATED OPERATIONS ● 6. INTEGRATED COMMUNICATIONS ●

TRIAL OVERVIEW: HotZone 4010 is a ruggedized outdoor wireless router which provides an ad hoc network infrastructure for voice, video and data applications. HotZone is a flexible wireless platform approach that provides more than five different applications or combinations. The system seamlessly bridges WiMAX, WiFi, 4.9GHz public safety, long-range 900MHz (NLOS) DECT and GSM/UMTS, with ability to rapidly incorporate evolving standards. HotZone radios support a multitude of applications and are fully upgradeable. HotZone provides a low cost communications and data retransmission system that is easily transported, set-up and used in both fixed and mobile configurations providing first responders and units from the forward to rear areas access to secure and unsecured data as needed to conduct operations.

SPONSOR:
US Navy
LOCATIONS:
SPAWAR
PARTNERS:
none


Alternatively Backhaul can be done in GSM or UMTS (ad hoc backhaul)
GSM NETWORK
Hotzone Base Station
INTERNET
SIP or H323 SoftSwitch
Billing and administration for WiFi and DECT
Backhaul on either WiMax, WiFi, 900 MHz or 4.9 GHz Public Safety Frequencies
Hotzone Remote Repeater
PSTN/POTS
Hotzone Remote Base Station
Hotzone Remote Base Station
DECT Data
Hotzone CPE
Hotzone CPE
DECT Phones
WiFi Enabled Device 2.4 or 5 GHz
Meshed Data Sensors Network
Fixed Wireless
Video Surveillance

ASSESSMEMT RESULTS:
During CWID 2007, the HotZone Trial operated on the HS/HD domain and received a Warfighter, Technical Interoperability, and a Conceptual Information Assurance (IA) assessment.

■ HotZone met CWID Objectives 3 and 6. It provided first responders a network infrastructure for voice, video, and data applications. First responders communicated using HotZone's voice/talk capability and successfully exchanged text files through HotZone's Digital Enhanced Cordless Telecommunications phones.

■ HotZone transmitted and delivered live video through its wireless application. The video scanned an area every 10 minutes and provided continuous surveillance of designated areas.

■ Stored video, utilized to simulate first responder communications, was clear and viewable, but email download times were lengthy due to the 5 megabyte file size.

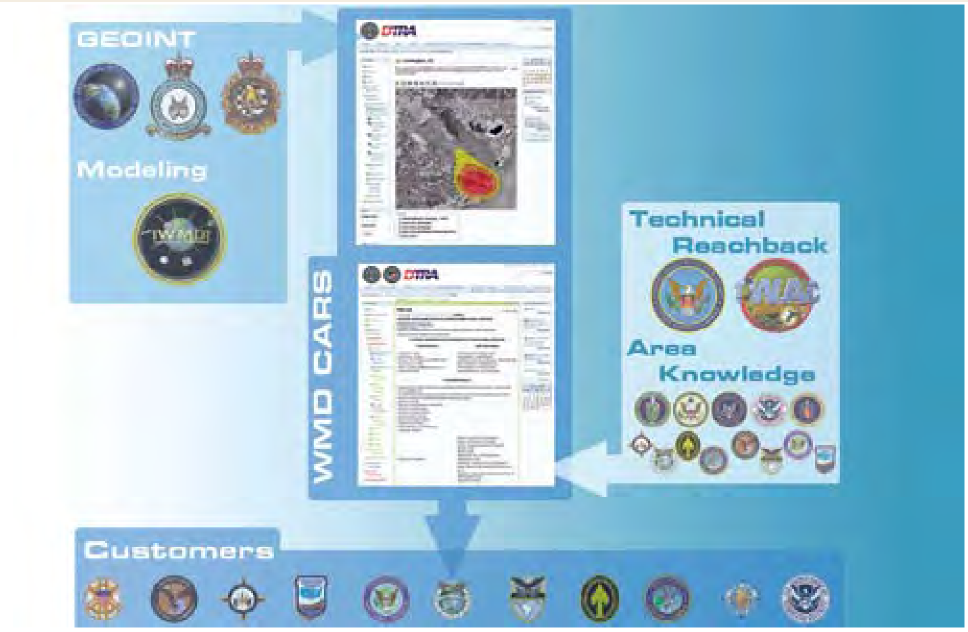
IT 6.53 UNABRIDGED ASSESSMENT LINK

Weapons of Mass Destruction Collaborative Advisory and Response System

3. INTEGRATED OPERATIONS ● 5. INTEGRATED PLANNING ●

TRIAL OVERVIEW: WMD CARS enables unprecedented collaboration between DTRA subject matter experts and combatant command/Joint Task Force (JTF) staffs. WMD CARS fuses dissimilar, critical information and distributes it to the strategic decision maker to support consequence management, force protection, and Military Assistance to Civil Authorities (MACA) in the event of hostile chemical, biological, radiological and nuclear (CBRN) events. This information sharing tool is a multi-use open-framework resource for deliberate and crisis action planning, at strategic and operational levels, that provides a clearer view of the battlefield to the warfighter.

SPONSOR:
Defense Threat Reduction Agency (DTRA)
LOCATIONS:
USEUCOM
USNORTHCOM
SPAWAR
ESC Hanscom
PARTNERS:
none



ASSESSMEMT RESULTS:
During CWID 2007, the WMD CARS II Trial operated on the CTF domain and received a Warfighter and Technical Interoperability assessment.

■ WMD CARS successfully met CWID Objectives 3 and 5. Using a web-based portal, WMD CARS provided DTRA analysts the tools to generate Request for Information (RFI) responses, and provided the ability to deliver data back to the requester without leaving the portal environment.

■ Using WMD CARS, DTRA analysts created OTH GOLD messages with plume information then inserted and emailed the message to the GCCS TOPCOP. The GCCS TOPCOP Manager processed and displayed the plume as an overlay on the TOPCOP.

■ WMD CARS timely information dispersion was useful for quickly deploying first responders.

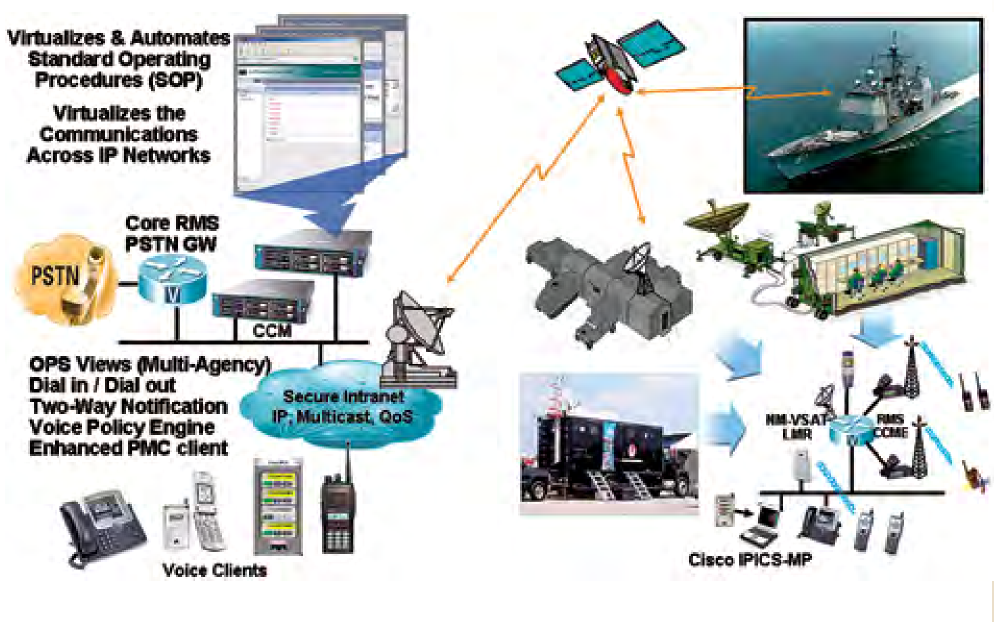
IT 6.66 UNABRIDGED ASSESSMENT LINK

Internet Protocol Interoperability and Collaboration System

6. INTEGRATED COMMUNICATIONS ●

TRIAL OVERVIEW: IPICS delivers secure, reliable communications at the point of necessity and empowers agencies to collaborate and coordinate across even the most formidable geographies and resource barriers. Agencies need flexible command and control – centralized or remote – improved response time and collaboration with other agencies, and real-time communications between diverse services. IPICS delivers: enhancements to existing applications, equipment and networks; an IP network-based solution providing rugged reliability and IP standards; and integrates voice, video and data.

SPONSOR:
Canada
LOCATIONS:
USNORTHCOM
NSWC Dahlgren
Canada
PARTNERS:
none



ASSESSMENT RESULTS:
The CISCO IPICS Trial operated on the HS/HD domain, recieving a Basic Information Assurance (IA) assessment and a SEIWG evaluation.

- IPICS successfully met CWID Objective 6, enhancing coalition information and knowledge sharing by providing voice interoperability between disparate radios and other devices.
- Warfighters said IPICS worked well with basic operator training, It was easy to use, stable and reliable. Voice systems integration was seamless.
- IPICS enabled rapid deployment and management of disparate audio communications systems by streamlining operations and command and control while protecting investment in deployed radio networks and applications.
- IA scans discovered correctable open ports and protocols, unneeded accounts and unnecessary services noted for correction in future releases.

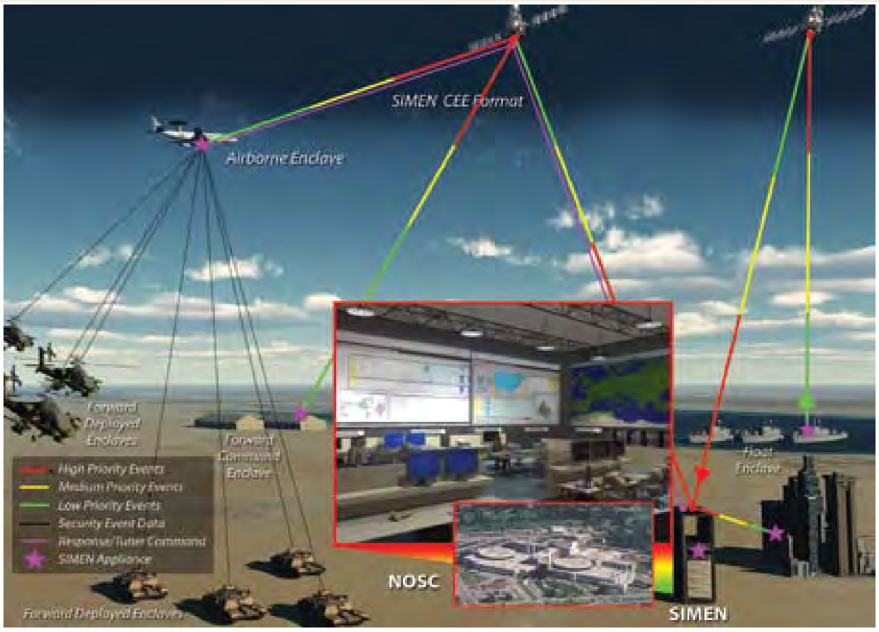
IT 6.74 UNABRIDGED ASSESSMENT LINK

Security Information Management for Enclave Networks

6. INTEGRATED COMMUNICATIONS ●

TRIAL OVERVIEW: The SIMEN prototype focuses on challenges associated with the ineffective collection of security event messages and the inefficient transport of such events to a centralized monitoring location. SIMEN's ultimate product is the bandwidth-efficient and secure transportation of relevant event messages in a network-sensitive manner. The SIMEN prototype receives local event data from the enclave sensor net, and reduces event size and volume by prioritizing, filtering, discarding, and queuing collected events. The results are forwarded, translated and send to the Network Operations and Security Center

SPONSOR:
US Air Force
LOCATIONS:
USNORTHCOM
ESC Hanscom
PARTNERS:
none



ASSESSMENT RESULTS:
During CWID 2007, the SIMEN Trial operated on the HS/HD domains and received a Technical Interoperability assessment.

- SIMEN successfully demonstrated CWID Objective 6 by automatically monitoring network activity at a network operations service centre and when required, successfully provided prioritized threat event messages to the SIMEN visualization machine. At the visualization machine, users could easily interpret messages and take appropriate action.
- SIMEN's event message prioritization can potentially be used in a bandwidth-constrained environment. During CWID execution, SIMEN was not in a bandwidth-constrained environment so this capability could not be measured or demonstrated.

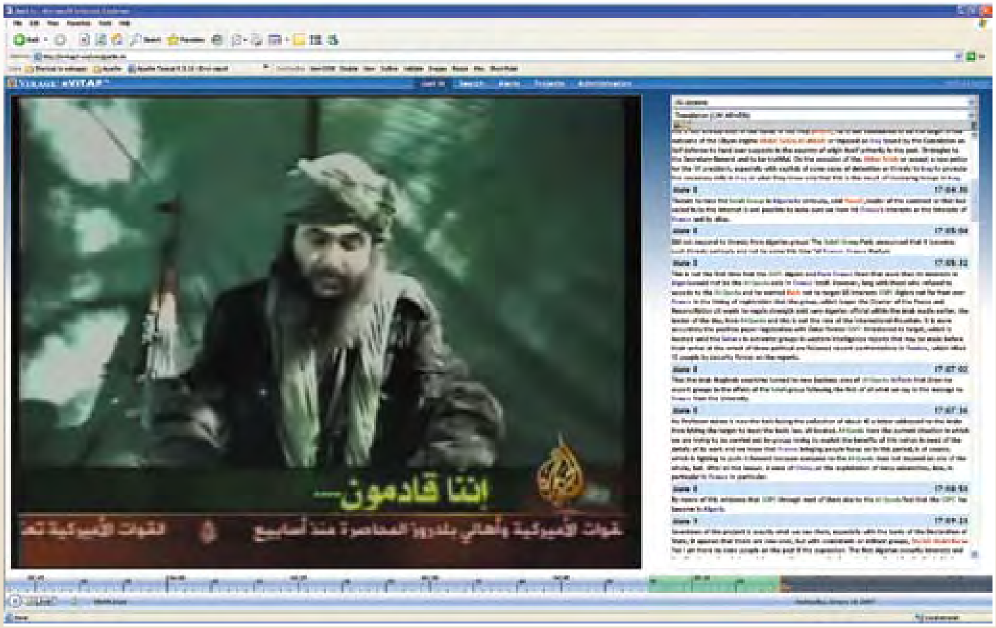
IT 6.89 UNABRIDGED ASSESSMENT LINK

Enhanced Video Text and Audio Processing

6. INTEGRATED COMMUNICATIONS ●

TRIAL OVERVIEW: eViTAP provides a fully automated, real-time, multilingual, news monitoring capability supporting over 20 languages including Arabic, Chinese, Japanese, Persian, and Russian. It uses a combination of advanced search and automated alerting to monitor multilingual news sources in real-time. Using state of the art technologies, eViTAP transcribes audio into text which is translated into English. Video and images are analyzed for face ID, logo detection, multilingual OCR, and closed captioning. Documents are translated into English and processed for automatic detection of people, places and organizations. eViTAP users leverage these powerful technologies via an intuitive, easy to use browser-based interface, presents a collaborative environment for quickly and efficiently finding, editing and exporting relevant intelligence.

SPONSOR:
US Joint Staff
LOCATIONS:
USNORTHCOM
NSWC Dahlgren
SPAWAR
Canada
New Zealand
PARTNERS:
none



ASSESSMEMT RESULTS:
eViTAP operated on the HS/HD domain, receiving Warfighter, Technical Interoperability, and Basic Information Assurance (IA) assessments.

- eViTAP successfully demonstrated CWID Objective 6, monitoring foreign broadcasts and processing Arabic language video, translating, and triggering relevant alerts. Users accessed video with English translation.
- Using eViTAPs key-word searches and e-mail alerts, warfighters monitored references to sensitive national security and returned alerts on foreign news broadcasts.
- Through live satellite video feeds, eViTAP provided operator alerts when data matched user-defined areas of interest, informing them of new relevant information and allowing efficient review of multiple translation inputs in a relatively short period.
- IA scans discovered correctable open ports and protocols, unneeded accounts and unnecessary services noted for correction in future releases.

IT 6.90 UNABRIDGED ASSESSMENT LINK

Optimized Data Environment for NetCentric Operations

6. INTEGRATED COMMUNICATIONS ●

TRIAL OVERVIEW: ODEN is universal software based advanced communications performance tool that provides 100% file transfer. The technology was developed, patented and employed with proven results since 2002. It provides improved performance over any media or network, improved bandwidth utilization, assures data integrity and data encryption and compression. ODEN is: a universal application for networks (RF, copper and fiber, at user, server, router or transmission level); media and hardware (Windows, Linux, Mac, Solaris OS's) neutral; is FISMA compliant; and DICOM implemented in OSI applications level seven. ODEN is also ACR and NEMA compliant.

SPONSOR:
USCENTCOM
LOCATIONS:
USNORTHCOM,
NSWC Dahlgren
SPAWAR
PARTNERS:
none

ODEN
Optimized Data Environment for NetCentric Operations

☑ Federal Information Security Management Act (FISMA) compliant
☑ Electromagnetic Interference/Compatibility (EMI/EMC) neutral
☑ Network or Peer-to-peer transmission tools
☑ Data compression factor of 2x - 20x
☑ Improved bandwidth utilization
☑ Optional encryption algorithm (8192 bit SSL or up to 2048 Elliptic Curve) by FIPS 113, 140-2, 180-2 and 197
☑ Improved performance over any media or network
☑ Universal application - network, media, and hardware neutral
☑ Windows, Linux, Mac & Solaris operating systems

ASSESSMENT RESULTS:
During CWID 2007, the ODEN Trial operated on the CTF and HS/HD domains and received a SEIWG evaluation.

- ODEN was moderately successful in meeting CWID Objective 6. While ODEN provides an innovative solution for compressing and transmitting data, user interfaces require more development.
- Transmission of large data files, imagery, and video files without absorbing vast amounts of bandwidth required careful control of transmission compression levels during transfer. This functionality requires more software implementation development relative to data transfer priorities in accordance with operational CONOPs and SOPs.
- ODEN garners bandwidth savings of modified files by exclusively transmitting the differences between previously sent data, image, or video files.

HISTORY OF CWID

CWID traces more than 16 years of history to establishment of the Secure Tactical Data Network (STDN) series originated by the U.S. Army to demonstrate emerging command, control, communications and computer (C4) capabilities.

STDN 1 and 2 concentrated on Army-only issues while STDN 3 brought the first multi-service participation. The Joint Staff recognized that advances in communications and information technology in the public sector were outpacing Department of Defense (DoD) capabilities.

The Joint Staff assumed sponsorship of the STDN series in 1993 under the C4I for the Warrior concept. The Defense Information Systems Agency (DISA) was directed to be Executive Agent, in concert with a lead Service, to organize network experiments, bringing emerging public sector and other government agency technologies into DoD projects and into war-fighters' sphere of recognition. DISA was also directed to improve joint C4 interoperability.

In 1994, annual STDN efforts evolved into the first Joint Warrior Interoperability Demonstration (JWID). The Air Force was lead service and U.S. Atlantic Command was host combatant command. The idea of moving from a static, one-dimensional picture of the battlefield to a near real-time, multi-dimensional battlespace picture became reality to joint and combined warfighters.

Key efforts in JWID '94 included demonstration of baseline segments of what became the Global Command and Control System (GCCS). Six weeks after the conclusion of JWID '94, GCCS was operationally deployed to U.S. Atlantic Command supporting military operations in Haiti. Full operational deployment of GCCS to all combatant commanders occurred within 12 months after JWID '94.

In 1997, the Chairman of the Joint Chiefs of Staff mandated interoperability in Joint Vision 2010, envisioning future conflicts as coalition operations. JWID assisted that vision, establishing itself as a coalition interoperability forum through invitations to Combined Communications Electronics Board (CCEB) nations (Australia, Canada, New Zealand and the United Kingdom) and NATO beginning with JWID '94 and continuing to the present. While invited participants used JWID to perform their own technology demonstrations and joint interoperability trials, their main intent was to promote and ensure C4 interoperability with the U.S.

EXPANSION

In 1998, JWID evolved into a two-year process to pursue selection and limited fielding of C4 technologies to warfighting combatant commanders. The Theme (first) Year conducted demonstrations and interoperability trials and selected "Gold Nuggets" for support and continued improvement during the Exploitation (second) Year, with eventual fielding to combatant commands. JWID '98 fielded three Gold Nuggets to warfighters.

U.S. Y2K concerns drove JWID '99-R to focus only upon coalition interoperability trials between the U.S. and CCEB/NATO nations.
To more easily promote trials and other Command, Control, Communications, Computers and Intelligence (C4I) experiments, the Coalition Wide Area Network (CWAN), established annually for JWID, evolved into the standing Combined Federated Battle Laboratories Network (CFBLNet). The network permits C4I experimentation among the U.S. and nations of CCEB/NATO year-round, using systems jointly owned and managed by CFBL membership.

JWID '00-'01 restored the two-year cycle, with 23 U.S. demonstrations and 145 combined/coalition demonstrations worldwide. Two Gold Nuggets were fielded in 2001. In addition, a Distributed Collaborative Tool Set (DCTS, now Defense Collaboration Tool Suite) was refined and subsequently selected for worldwide fielding to the Unified Commands. DISA fielded the capability, within 72 hours, in support of the Office of the Secretary of Defense (OSD) requirements following terrorist attacks of September 11th,
to multiple DoD networks.

COALITION INTEROPERABILITY

JWID 2002 featured transition from a limited fielding of technology to full focus on coalition interoperability, led by U.S. Pacific Command (USPACOM), the host combatant command. The demonstration included Pacific Rim nations in a Pacific Theater Initiative (PTI), with Japan, South Korea, Singapore, and Thailand participating while Malaysia and the Philippines observed operations. Coalition partners were integrated on the Multinational Task Force (MTF) and component staffs to maximize opportunities. The JWID CWAN continued use of CFBLNet architecture and services established in past demonstrations. U.S. Joint Forces Command (USJFCOM) fielded a JWID demonstrated language translation device.

JWID 2003 took coalition interoperability to new heights. USPACOM guided the CTF and, for the first time, Japan, South Korea, Thailand and Singapore provided staffing to expand information exchange over dual domains. One key focus for 2003 included management of information exchange between the traditional 6-eyes network to a larger, more robust 10-eyes network. The larger network was vital to JWID's success because Pacific Rim nations needed effective information to serve in MTF staff positions. JWID 2003 addressed multi-level security technical solutions and refinement of coalition policies and procedures to overcome issues surrounding information exchange.

DISA assumed duties as the lead agency, providing broad-base management support of JWID activities. Four Coalition Interoperability Trials (CITs) with especially noteworthy performance were submitted to USJFCOM J861, for consideration for limited fielding.

HOMELAND SECURITY

JWID 2004 featured U.S. Northern Command (USNORTHCOM) as the host combatant command. USNORTHCOM brought a Homeland Security/Homeland Defense (HS/HD) focus to the demonstration, breaking new ground beyond the traditional JWID coalition interoperability area. USNORTHCOM invited agencies within the Department of Homeland Security, including first-time participation for the Federal Emergency Management Agency (FEMA), the Federal Bureau of Investigation (FBI), the U.S. Coast Guard, and the National Guard Bureau. Limited coalition participation among these organizations occurred as Public Safety and Emergency management Canada (PCEPC) joined in the interoperability trials, beginning significant potential for more extensive cooperation among other coalition homeland security organizations and their U.S. counterparts. USJFCOM filled an ancillary role, assisting with select fielding of technologies to combatant commanders. JWID 2004 involved 25 countries, military services, and government agencies participating in a scripted scenario over a global network.

USNORTHCOM was host Combatant Command in 2005 as the demonstration moved forward with a name change. Now the Coalition Warrior Interoperability Demonstration (CWID), the shift from "Joint" to "Coalition" describes the larger community of participants, including national and international government agencies.

USJFCOM formally assumed oversight for planning and execution of CWID 2005 from the Joint Staff in July 2004. This involvement brings USJFCOM advocacy for U.S. combatant command interoperability shortfall resolution to the forefront. USJFCOM's objectives include (1) to ensure CWID demonstrates relevant technologies that address combatant commander's capability gaps, (2) to investigate military, coalition and interoperability solutions and (3) to identify technologies suitable for prototype initiatives.

Fifteen trials were considered "success stories," moving forward for continued development. Seven ITs were selected for Service, Agency, or limited Combatant Commander fielding (including fielding in support of Hurricane Katrina). Two ITs achieved milestones and continue spiral development as Programs of Record. One was selected for funding via a Congressional Plus-up for further research and development, and one was submitted as a Limited Acquisition Authority candidate. Four others were identified for agency fielding in some capacity.

THE LARGER COALITION

U.S. European Command (USEUCOM) assumed host combatant command for 2006 through 2008. USNORTHCOM continues as the lead for HS/HD CWID operations.

Out of 34 trials in CWID 2006, USJFCOM published 12 U.S. and three coalition trials with potential to answer combatant-commander defined objectives. Four promising technologies were sponsored by USNORTHCOM.

The HS/HD site orchestrated a first live exercise associated with CWID, involving local Colorado Springs first responders. The Marine Corps and Army site, Dahlgren, Va., linked that portion of the scenario into Coalition Task Force operations over the CWID network.

USEUCOM coalition participants drove development of a multi-tier network to access HS/HD networks while still operating in the Coalition Task Force military scenario. Canada and USEUCOM joined the HS/HD enclave to fully participate in trial test and evaluation.

NATO used CWID 2006 to advance Transformation within the Alliance. The NATO Response Force (NRF), designed to be agile, joint and expeditionary, participated as a Coalition entity in the scenario for the first time. CWID provided a network to explore a robust and flexible Computer Information Systems (CIS) environment, key to the NRF concept.

USJFCOM plans to assume combatant command leadership for 2009 and 2010.

TRIAL HIGHLIGHTS 2006

PIPELINE TECHNOLOGIES AND OUTCOMES

■ Four trials were Programs of Record (POR) conducting spiral development:

1. Integrated Information Management Systems (IIMS): was a U.S. Air Force/AFRL R&D effort that continues spiral development in 2007; involved in transition agreements with JWARN and JEB PORs

2. Coalition & Civil Agency Capable Wireless Information Transfer System (C3WITS): highly successful technology that was considered for further devlopment after the demonstration

3. Intelligent Road/Rail Information Server (IRRIS): U.S. Army sponsored technology and POR; government owned; expanded utility to include U.S. Transportation Command (USTRANSCOM)

4. HLS/D Collaborative Information Exchange Environment (CIEE): NGB sponsored POR; continuing spiral development in 2007 as Joint Collaborative Information Exchange Environment

■ One trial a System of Record conducting spiral development:

1. Wide Area Interoperability System (WAIS) & ACU 1000: sponsored by USNORTHCOM; successfully demonstrated stated objectives; picked-up on the GSA schedule; Department of Homeland Security (DHS) and Federal Emergency Management Agency (FEMA) purchased technology as core of Mobile Disaster Response Vehicles

■ Two demonstrations picked up for purchase:

1. Incident Commander's Radio Interface (ICRI): technology participated as a trial in 2005; demonstrated at Dahlgren during 2006; real-world success in Katrina crisis response; purchased by U.S. Marine Corps and DHS for disaster response

2. "Buster:" UAS late entry in 2006; demonstrated well at Dahlgren; units purchased by U.S. Marine Corps and United Kingdom for immediate training and deployment

TRIAL HIGHLIGHTS 2005

PIPELINE TECHNOLOGIES AND OUTCOMES

■ One trial Limited Acquisition Authority (LAA) candidate:

1. Multi-level-secure Information Infrastructure (MI2): considered by USNORTHCOM for submission as Urgent Need Statement (UNS), LAA request; U.S. Joint Forces Command (USJFCOM)/Joint Systems Integration Command (JSIC) military utility assessment; USNORTHCOM chose not to submit UNS; LAA did not go forward at USJFCOM

■ Two trials targeted for further testing:

1. Advanced Geospatial Imagery Library Enterprise (AGILE): further development by National Geospatial-Intelligence Agency (NGA) into a near-term operational capability; currently being assessed by JSIC as part of the JBSA initiative; included as baseline technology for transmitting imagery

2. Posted Applications Over Return Channel Satellite: Global Broadcast System (GBS) continues spiral development in JUICE 06; DoD POR that supports service interests in field today

■ One trial funding identified, Congressional Plus-up:

1. Masking Shunt: funded for continued ONR evaluation; received second year of congressional funding for continued testing at JSIC

■ Three trials are Programs of Record:

1. Commercial Joint Mapping Tool Kit (CJMTK): CWID venue used successfully for spiral development

2. Joint Warning and Reporting Network (JWARN): CWID used successfully for spiral development; has successfully completed a JSIC planned assessment as part of DJC2 GCCS 4.0 Interoperability Demo

3. Joint Tactical COP Workstation (JTCW): CWID venue used successfully for spiral development

■ Two trials used in U.S. hurricane relief efforts:

1. Incident Commanders' Radio Interface (ICRI): USNORTHCOM and numerous civil law enforcement activities purchased technology in support of HS/HD; U.S. Marine Corps purchased and installed ICRI in Rapid Response Vehicles to interface with civil authorities in the event of a crisis response; ICRI used effectively to support Katrina relief efforts; U.S. Marine Corps and DHS fielded units following 2006 demonstration

2. ARINC Wireless Interoperability Solution (AWINS): used effectively to support hurricane Katrina relief effort; gone on to commercial success outside of DoD

■ Two trials proposed for limited combatant commander fielding:

1. Multi-Level Chat (MLC): continues JSIC evaluation under Automated Information Security (AIS) umbrella; proposed fielding in response to Urgent Need Statement (UNS), IRAQ; approved by DSAWG for use in Trident Warrior and retention by Navy thereafter for operational use

2. One Way File Transfer (OWFT): continues JSIC evaluation under AIS umbrella for proposed fielding in response to U.S. Central Command (USCENTCOM) UNS in IRAQ proposed for CENTCOM; latest version in NSA Certification, Test & Evaluation; continues

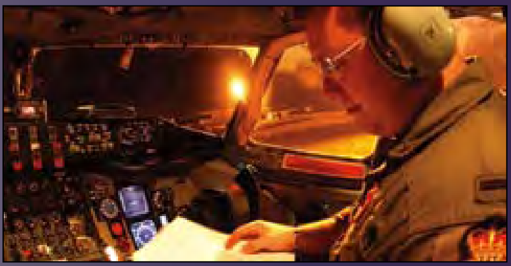
■ Two trials had limited U.S. Marine Corps/Service fielding:

1. Tactical Medical Coordinating System (TacMedCS): deployed to IRAQ to support operations

2. Marine Air-Ground Task Force Continuity of Operations System (MAGTFCS): deployed to IRAQ to support ongoing operations

■ One trial for agency fielding

1. Pliable Display Technology: NGA prototype, developed as a near-term operational capability, now fielded



2008 Objectives

For more detailed objective explanations and additional information regarding CWID 2008, refer to the Federal Business Opportunities (FBO) and other resources on the demonstration website.

OBJECTIVE 1

IMPROVE COALITION AND JOINT C4ISR ARCHITECTURE

■ Enhance leadership's capability to command, control and coordinate across joint and coalition forces, government agencies, non-governmental organizations (NGOs) and first responders.

OBJECTIVE 2

IMPROVE INFORMATION SHARING ACROSS THE FULL RANGE OF MILITARY OPERATIONS

■ Provide the capability to share information across multiple networks of potentially different security classifications and caveats. Emphasis should be on passing information to both U.S.-controlled, coalition networks such as U.S. Central Command's Combined enterprise Regional Information Exchange System (CENTRIXS) and coalition/alliance controlled networks such as NATO's Initial Data Transfer System (NIDTS), NATO Mission Wide Area Network (WAN), or releasable to Republic of Korea (RELROK). Data sharing encompasses the need for cross-domain solutions (CDS) and the assurance that information passed through CDS can be utilized by systems within all security enclaves.

OBJECTIVE 3

ENHANCE CROSS-DOMAIN AND MULTIPLE SECURITY LEVEL INFORMATION EXCHANGE TOOLS

■ Provide solutions that improve the commander's ability to share intelligence information products (documents, images, databases, etc.) with coalition partners, including joint and coalition forces, government agencies, NGOs and first responders.

OBJECTIVE 4

ENHANCE INTEGRATED LOGISTICS PLANNING TOOLS

■ Demonstrate the ability to access, consolidate and display logistical information to include movement, location and status of joint forces, military services, interagency, coalition, NGO, first responders as well as equipment and supplies in near real time across organizational boundaries.

OBJECTIVE 5

ENHANCE GOVERNMENT AGENCY INTEROPERABILITY

■ Provide solutions that improve a Combatant Commander's ability to conduct collaborative planning with coalition partners, including joint and coalition forces, government agencies, NGOs and first responders. Focus is on enhanced collaboration and engendering a "need to share" vice a "need to know" culture.

www.cwid.js.mil